

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
Naoya TAKAO et al. :
Serial No. NEW : **Attn: APPLICATION BRANCH**
Filed July 22, 2003 : Attorney Docket No. 2003_1017A
TERMINAL APPARATUS, COMMUNICATION
METHOD, AND COMMUNICATION SYSTEM THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450


Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-213401, filed July 23, 2002, and Japanese Patent Application No. 2002-300108, filed October 15, 2002, as acknowledged in the Declaration of this application.

Certified copies of said Japanese Patent Applications are submitted herewith.

Respectfully submitted,

Naoya TAKAO et al.

By 

Michael S. Huppert
Registration No. 40,268
Attorney for Applicants

MSH/kjf
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 22, 2003

日 本 国 特 許 庁

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 7月23日

出 願 番 号

Application Number:

特願2002-213401

[ST.10/C]:

[JP2002-213401]

出 願 人

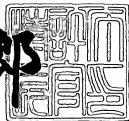
Applicant(s):

松下電器産業株式会社

2003年 6月12日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3045987

【書類名】 特許願

【整理番号】 2032740081

【提出日】 平成14年 7月23日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 ▲たか▼尾 直弥

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 杉山 圭司

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 森 俊也

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 グループ管理方法、グループ管理システム、グループ管理プログラム、およびグループ管理プログラムを記録した記録媒体

【特許請求の範囲】

【請求項1】 自分の公開鍵と秘密鍵を保持している加入依頼者が一人以上のメンバから構成されるグループにネットワークを介して新規加入するためのグループ加入方法であって、前記グループ固有の秘密鍵と公開鍵を保持する管理者に対して前記加入依頼者が少なくとも自分の公開鍵を送付して前記グループへの加入を依頼する加入依頼ステップと、前記管理者が少なくとも前記加入依頼者の公開鍵と前記グループ固有の秘密鍵に基づいて作成したグループ参加証を前記加入依頼者に送付する参加証発行ステップと、を実行することを特徴とするグループ加入方法。

【請求項2】 前記加入依頼ステップの前に前記管理者が偽者でないことを前記加入依頼者が確認する管理者確認ステップを実行することを特徴とする請求項1記載のグループ加入方法。

【請求項3】 前記加入依頼ステップにおいて前記加入依頼者が前記管理者に対して自分自身を特定する情報を追加して送付し、前記管理者が前記加入依頼者を特定する情報に基づき前記加入依頼者を加入させるか否かを判断する加入判断ステップを前記参加証発行ステップの前に実行することを特徴とする請求項1または請求項2に記載のグループ加入方法。

【請求項4】 第1から第3の請求項記載のグループ加入方法により前記グループ参加証を取得したメンバ間で前記グループへの加入資格を認証するためのグループ認証方法であって、認証者が被認証者に対して認証用文字列を送付する認証開始ステップと、前記被認証者が前記認証者に対して少なくとも前記認証用文字列から自分の秘密鍵に基づいて作成した応答文字列と前記グループ参加証を送付して認証を依頼する認証依頼ステップと、前記認証者が前記グループ参加証から前記グループ固有の公開鍵に基づいて前記被認証者の公開鍵を得て、次に前記応答文字列と前記被認証者の公開鍵から前記認証用文字列に一致する文字列が得られることを確認することをもって前記被認証者が前記グループの加入者である

ことを認証する認証ステップと、を実行することを特徴とするグループ認証方法

【請求項5】 前記認証ステップの後に、前記認証者と前記被認証者が立場を入れ替えて前記グループ認証開始ステップから前記認証ステップまでを実行することを特徴とする請求項4記載のグループ認証方法。

【請求項6】 前記参加証発行ステップにおいて前記管理者が少なくとも前記加入依頼者の公開鍵、前記グループ参加証の有効期限に関する情報および前記グループ固有の秘密鍵に基づいて作成したグループ参加証を作成し前記加入依頼者に送付することを特徴とする請求項1から請求項3のいずれか1項に記載のグループ加入方法。

【請求項7】 前記認証ステップにおける前記被認証者の認証の際に、前記グループ参加証に含まれる有効期限に関する情報に基づいて前記被認証者が前記グループの有効な加入者であるかどうかを判断することを特徴とする請求項4または請求項5に記載のグループ認証方法。

【請求項8】 請求項6記載のグループ加入方法により前記グループ参加証を取得したメンバが前記グループ参加証の有効期限に関する情報を更新するためのグループ参加証更新方法であって、前記更新依頼者が前記管理者に対して少なくとも前記グループ参加証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する参加証更新依頼ステップと、前記管理者が前記グループ参加証から前記グループに固有の公開鍵に基づいて前記更新依頼者の公開鍵を得て、前記更新依頼者の公開鍵と新たな前記有効期限に関する情報および前記グループ固有の秘密鍵に基づいて作成した新たな前記グループ参加証を前記更新依頼者に送付する参加証更新ステップと、を実行することを特徴とするグループ参加証更新方法。

【請求項9】 前記参加証更新依頼ステップの前に前記管理者が偽者でないことを前記更新依頼者が確認する第2の管理者確認ステップを実行することを特徴とする請求項8記載のグループ参加証更新方法。

【請求項10】 前記管理者が前記グループ参加証発行の権限を持つ発行者を追加する方法であって、発行者候補のメンバが少なくとも自分の公開鍵を前記管

理者へ送付する発行者鍵送付ステップと、前記管理者が少なくとも前記発行者候補の公開鍵と前記グループ固有の秘密鍵に基づいてグループ参加証発行許可証を作成し前記発行候補者に送付する参加証発行許可証発行ステップとを実行することを特徴とする発行者追加方法。

【請求項11】 自分の公開鍵と秘密鍵を保持している加入依頼者が請求項10記載の発行者追加方法により前記管理者からグループ参加証発行許可証の発行を受けた発行者からグループ参加証の発行を受ける第2のグループ加入方法であって、前記加入依頼者が少なくとも自分の公開鍵を送付して前記グループへの加入を依頼する第2の加入依頼ステップと、前記発行者が少なくとも前記加入依頼者の公開鍵と前記発行者の秘密鍵に基づいて作成したグループ参加証および前記発行者の前記グループ参加証発行許可証を前記加入依頼者に送付する第2の参加証発行ステップと、を実行することを特徴とする第2のグループ加入方法。

【請求項12】 前記第2の加入依頼ステップの前に前記発行者が偽者でないことを前記加入依頼者が確認する発行者確認ステップを実行することを特徴とする請求項11記載の第2のグループ加入方法。

【請求項13】 前記第2の加入依頼ステップにおいて前記加入依頼者が前記発行者に対して自分自身を特定する情報を追加して送付し、前記発行者が前記加入依頼者を特定する情報に基づき前記加入依頼者を加入させるか否かを判断する第2の加入判断ステップを前記第2の参加証発行ステップの前に実行することを特徴とする請求項11または請求項12に記載の第2のグループ加入方法。

【請求項14】 請求項11から請求項13のいずれか1項に記載の第2のグループ加入方法により前記グループ参加証を取得したメンバー間で前記グループへの加入資格を認証するための第2のグループ認証方法であって、認証者が被認証者に対して認証用文字列を送付する第2の認証開始ステップと、前記被認証者が前記認証者に対して少なくとも前記認証用文字列から自分の秘密鍵に基づいて作成した応答文字列と前記グループ参加証および前記グループ参加証発行許可証を送付して認証を依頼する第2の認証依頼ステップと、前記認証者が前記グループ参加証発行許可証から前記グループ固有の公開鍵に基づいて前記発行者の公開鍵を得て、次に前記グループ参加証から前記発行者の公開鍵に基づいて前記被認証

者の公開鍵を得て、さらに前記応答文字列と前記被認証者の公開鍵から前記認証用文字列に一致する文字列が得られることを確認することをもって前記被認証者が前記グループの加入者であることを認証する第2の認証ステップと、を実行することを特徴とする第2のグループ認証方法。

【請求項15】 前記第2の認証ステップの後に、前記認証者と前記被認証者が立場を入れ替えて前記第2のグループ認証開始ステップから前記第2の認証ステップまでを実行することを特徴とする請求項14記載の第2のグループ認証方法。

【請求項16】 前記第2の参加証発行ステップにおいて、前記発行者が少なくとも前記加入依頼者の公開鍵、前記グループ参加証の有効期限に関する情報および前記発行者の秘密鍵に基づいて作成したグループ参加証を作成し前記加入依頼者に送付することを特徴とする請求項11から請求項13のいずれか1項に記載の第2のグループ加入方法。

【請求項17】 前記第2の認証ステップにおいて前記グループ参加証に含まれる有効期限に関する情報に基づいて前記被認証者が前記グループの有効な加入者であるかどうか判断することを特徴とする請求項14または請求項15に記載の第2のグループ認証方法。

【請求項18】 請求項16記載の第2のグループ加入方法により前記グループ参加証を取得したメンバが前記グループ参加証の有効期限に関する情報を更新するための第2のグループ参加証更新方法であって、前記更新依頼者が前記発行者に対して少なくとも前記グループ参加証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する第2の参加証更新依頼ステップと、前記発行者が前記グループ参加証発行許可証から前記グループに固有の公開鍵に基づいて前記グループ参加証発行許可証を発行した発行者の公開鍵を得て、次に前記グループ参加証から前記グループ参加証発行許可証を発行した発行者の公開鍵に基づいて前記更新依頼者の公開鍵を得て、さらに前記更新依頼者の公開鍵と新たな前記有効期限に関する情報および前記発行者の秘密鍵に基づいて作成した新たな前記グループ参加証を前記更新依頼者に送付する第2の参加証更新ステップと、を実行することを特徴とする第2のグループ参加証更新方法。

【請求項 19】 前記第 2 の更新依頼ステップの前に前記発行者が偽者でないことを前記更新依頼者が確認する発行者確認ステップを実行することを特徴とする請求項 18 記載の第 2 のグループ参加証更新方法。

【請求項 20】 前記参加証発行許可証発行ステップにおいて、前記管理者が少なくとも前記発行者候補の公開鍵、前記グループ参加証発行許可証の有効期限に関する情報および前記グループ固有の秘密鍵に基づいてグループ参加証発行許可証を作成し前記発行者候補者に送付することを特徴とする請求項 10 記載の発行者追加方法。

【請求項 21】 前記第 2 の加入依頼ステップの前に前記グループ参加証発行許可証に含まれる有効期限に関する情報に基づいて前記発行者の前記グループ参加証発行許可証が有効かどうか判断することを特徴とする請求項 11 から請求項 13 または請求項 16 のいずれか 1 項に記載の第 2 のグループ加入方法。

【請求項 22】 前記第 2 の認証ステップにおいて前記グループ参加証発行許可証に含まれる有効期限に関する情報に基づいて前記被認証者が所有する前記グループ参加証発行許可証が有効かどうか判断することを特徴とする請求項 14 または請求項 15 または請求項 17 に記載の第 2 のグループ認証方法。

【請求項 23】 請求項 10 記載の発行者追加方法により前記グループ参加証発行許可証の発行を受けた前記発行者が前記グループ参加証発行許可証の有効期限に関する情報を更新するための発行許可証更新方法であって、前記発行者が前記管理者に対して少なくとも前記グループ参加証発行許可証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する発行許可証更新依頼ステップと、前記管理者が前記グループ参加証発行許可証から前記グループに固有の公開鍵に基づいて前記発行者の公開鍵を得て、前記発行者の公開鍵と新たな前記有効期限に関する情報および前記発行者の秘密鍵に基づいて作成した新たな前記グループ参加証発行許可証を前記発行者に送付する発行許可証更新ステップと、を実行することを特徴とする発行許可証更新方法。

【請求項 24】 前記発行許可証更新依頼ステップの前に、前記管理者が偽者でないことを前記発行者が確認する第 3 の管理者確認ステップを実行することを特徴とする請求項 23 記載の発行許可証更新方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークで接続された機器を使う複数のユーザがグループを構成し、情報をグループ内でのみ安全に共有するためのグループ管理方法に関する。

【0002】

【従来の技術】

インターネットに接続してネットワークサービスを楽しむユーザ数は、接続機器や接続料金の廉価化、接続機器の多彩化、および通信速度の向上などにより、急速に増加している。インターネット普及当初は、一部の情報提供者が提供する情報を一般ユーザがダウンロードする一方のサービスが主流であったが、現在は自分の持つ情報、すなわちテキストデータ、静止画像データ、音声データ、動画データなどを発信したいという一般ユーザも増え、主にWWW (World Wide Web) などのサーバに自分の情報を複製し、他のユーザが閲覧可能とすることによってこれを実現している。

【0003】

サーバで情報を公開するにあたっては、大きく分けて(1)サーバを自分で運用する、(2)サービス提供者が有料または無料で提供しているサーバに情報をアップロードする、という二つの方法がある。さらに、不特定多数を対象に発信するのではなく、友人・家族・共通の趣味を持つ者など特定ユーザ間(以下グループと呼ぶ)でのみプライベートな情報を共有したいという要求も増えているが、これを実現する方法としては、主に認証サーバを用いる方法すなわちグループへの参加を認められたユーザのユーザIDとパスワードの組(以下グループリスト)を認証サーバ(情報提供サーバと同一であっても良い)に登録しておき、ユーザが入力したユーザIDとパスワードの組を確認することによって当該グループでの情報共有を許可する方法などが用いられている。

【0004】

このように情報提供者はサーバに情報を格納しておき、情報受信者がサーバへ

アクセスするというモデル（サーバクライアントモデルと呼ぶ）には、次の問題点がある。すなわち、自分でサーバで運用する場合には、（１）高度な知識が必要：サーバやネットワーク等に関する十分な知識が必要とされ、一般ユーザが運用することは困難な場合が多い、（２）コストがかかる：機材やソフトウェア以外にも、基本的に常時サービスを提供するためにサーバを常時稼働させるための運用費が必要となる、などの問題点があり、有料または無料で提供されるサーバを利用する場合には、（３）容量制限：多くの場合サーバに格納できる情報の容量には制限が設けられており、有料サーバの場合はコストをより多く負担することで容量制限を緩和することができるが、その場合にはより多くのコストがかかる、（４）プライバシー：サーバ提供者が信頼に足る場合であっても、何らかの事故等でサーバに格納した情報が第三者に漏れる場合があり、真にプライバシー保護を必要とする情報を共有することは困難である、などの問題点があり、共通の課題としては、（５）信頼性：サーバが何らかのトラブルでアクセス不能になった場合、情報発信や情報共有はまったく不可能となる、という問題点がある。なお、上で述べたコストに関する問題については、情報提供に対する収入によりコストを回収できるならば一定の負担は問題とならないが、一般ユーザが個人情報を発信あるいは共有する多くの場合はこれに当てはまらない。

【0005】

上記のようなサーバクライアントモデルにおける情報共有時の問題点を解消するために近年着目されているのがピアトゥーピア（Peer-to-Peer、以下P2P）モデルである。これは、情報をサーバに一極集中させず、必要ときに情報発信者-情報受信者間で直接伝送することで上記問題点を解決するものである。

【0006】

P2Pモデルのネットワーク（以下P2Pネットワーク）に参加しているユーザ間で情報を転送する場合の流れを図15にて例示する。各ユーザはP2Pネットワークに参加している他のユーザの存在を一人以上知っており、例えばAはBとF、BはAとCとD、EはDのみの存在を知っている。この状態でAが欲する情報を受信する際には、まず情報を持つユーザを特定するために検索を行う。

【0007】

Aはまず自分の知っているBとFに検索要求を発する。次にBとFはそれぞれが知っているユーザにこの検索要求を中継し、その先のユーザも同様に中継する（ステップ1501）。そしてこの検索要求に合致する情報を持っているユーザ、この場合はCとEは、Aに対して情報を持っていることを直接通知し（ステップ1502）、Aは何らかの判断基準でEを選択してAとEの間で情報の転送が直接行われる（ステップ1503）。もちろん情報を分割してCとEの両者から同時に転送することも可能である。

【0008】

これにより、前記サーバクライアントモデルの問題点（1）～（5）は次のように解決される。（1）サーバを運用しないため高度な知識は必要とされない。（2）またサーバを運用または利用するためのコストも不要である。（3）情報発信者Eから直接情報Aを受信するので、転送可能な情報の容量はAとEのローカルな記録容量のみに制約され、実質的に容量の制限はない。（4）転送される情報はAとE以外の第三者を経由しないので、既存技術でAとEの間の通信路を暗号化するなどすれば情報のプライバシーは保たれる。（5）仮にEがネットワークに参加していない状態（オフライン）であっても、AはCから必要な情報を得ることができる。

【0009】

さて、P2Pネットワークにおいてグループでの情報共有を行う場合には認証サーバが存在しないので、何らかの別の方法で各ユーザがそのグループに参加しているかどうかを互いに認証する必要がある。図16を用いてその実現例と課題を説明する。

【0010】

一つの方法はサーバクライアントモデルにおいて認証サーバが保持していたグループリストを当該グループに属する各ユーザが保持する方法である。図16（1）において、ユーザA、B、Cはそれぞれグループリストを保持していて、グループリストにはグループを構成するユーザ（メンバ）としてAとBとCが記述されている。各ユーザ、例えばCが自分のユーザIDとパスワードを他のユー

ザ（AかつまたはB）に知らせると、AかつまたはBはそのユーザIDとパスワードを自分が保持するグループリスト内の記述と比較する。比較結果が一致すればCはグループのメンバであると認証され、AかつまたはBとの間での情報共有を許可される。グループメンバではないユーザXはグループリストに含まれるユーザIDとパスワードを知らないので、A、B、Cとの間での情報共有は許可されず、A、B、Cからなるグループ内のプライバシーが保たれる。

【0011】

この第一の方法には次の問題がある。Cがオフライン時に、AまたはBがDを新たなメンバとしてグループに参加させたとする。その場合、図16（2）に示すようにA、B、Dは、DのユーザIDとパスワードの記述が追加された新たなグループリストを共有することになる。この時点でCはオフラインであるためこのグループリストの更新は通知されない。次にA、BがオフラインでC、Dのみがネットワーク参加状態（オンライン）になった場合（図16（3））、Cは自分の保持するグループリストにはDの記述がないためDがグループメンバであることを認証できず、共にグループメンバであるC、Dの間でグループの情報共有が不可能になる。（Dの保持するグループリストにはD自身の記述があるが、Dがグループリストを改ざんして追加した可能性があるためCはそれを信頼することはできない。）すなわち、この第一の方法では、グループリストを各ユーザがそれぞれ保持するが、その同期を保つことができないという問題点がある。

【0012】

この問題を防ぐ第二の方法はグループリストを特定のメンバー名のみが保持し、グループメンバの変更およびユーザのグループ参加状態の認証をこの特定メンバのみが行うことである。しかし、この第二の方法には、この特定メンバがオフラインの間は他のメンバ間で互いの認証ができなくなる問題がある。例えば図16（4）においてAがこの特定メンバであり、B、Cがグループメンバであるとする。Aがオンラインであれば、BはAに問い合わせることによりCがグループメンバであることを認証できる。しかし、図16（5）に示したようにAがオフラインの場合、BはAへの問い合わせが失敗するためCを認証できず、共にグループメンバであるBとCの間で情報共有が不可能となる。

【0013】

【発明が解決しようとする課題】

以上述べたように、サーバクライアントモデルの問題点を解決するためのP2Pネットワークにおいてグループでの情報共有を行う場合、(1)各ユーザがグループリストを保持する方法ではメンバ間のグループリストの同期が取れなくなる可能性がありその場合グループメンバ間であっても互いに認証することができないという問題点があり、また(2)特定メンバのみがグループリストを保持する方法ではその特定メンバがオフラインである間は他のメンバ間でグループメンバであることを互いに認証できなくなるという問題点がある。

【0014】

本発明は、上記問題点に鑑み、グループでの情報共有にサーバの運用を必要とせず、かつ任意のメンバ間で常にグループメンバであることの認証が常に可能なグループ管理方法を提供することを目的とする。

【0015】

【課題を解決するための手段】

本発明は、以上述べた課題を解決するため、以下のような構成をとるグループ加入方法、グループ認証方法、およびグループ参加証更新方法、ならびにこれらを含むグループ管理方法、グループ管理プログラム、およびこれを記録した記録媒体を提供する。または、発行者追加方法、第2のグループ加入方法、第2のグループ認証方法、第2のグループ参加証更新方法、および発行許可証更新方法、ならびにこれらを含むグループ管理方法、グループ管理プログラム、およびこれを記録した記録媒体を提供する。

【0016】

グループ加入方法の一実施形態は、自分の公開鍵と秘密鍵を保持している加入依頼者が一人以上のメンバから構成されるグループにネットワークを介して新規加入するためのグループ加入方法であって、前記グループ固有の秘密鍵と公開鍵を保持する管理者に対して前記加入依頼者が少なくとも自分の公開鍵を送付して前記グループへの加入を依頼する加入依頼ステップと、前記管理者が少なくとも前記加入依頼者の公開鍵と前記グループ固有の秘密鍵に基づいて作成したグルー

ブ参加証を前記加入依頼者に送付する参加証発行ステップと、を実行することを特徴とする。

【0017】

また、グループ加入方法の一実施形態においては、前記加入依頼ステップの前に前記管理者が偽者でないことを前記加入依頼者が確認する管理者確認ステップを実行することを特徴とする。

【0018】

また、グループ加入方法の一実施形態においては、前記加入依頼ステップにおいて前記加入依頼者が前記管理者に対して自分自身を特定する情報を追加して送付し、前記管理者が前記加入依頼者を特定する情報に基づき前記加入依頼者を加入させるか否かを判断する加入判断ステップを前記参加証発行ステップの前に実行することを特徴とする。

【0019】

また、グループ加入方法の一実施形態においては、前記参加証発行ステップにおいて前記管理者が少なくとも前記加入依頼者の公開鍵、前記グループ参加証の有効期限に関する情報および前記グループ固有の秘密鍵に基づいて作成したグループ参加証を作成し前記加入依頼者に送付することを特徴とする。

【0020】

グループ認証方法の一実施形態は、グループ加入方法により前記グループ参加証を取得したメンバー間で前記グループへの加入資格を認証するためのグループ認証方法であって、認証者が被認証者に対して認証用文字列を送付する認証開始ステップと、前記被認証者が前記認証者に対して少なくとも前記認証用文字列から自分の秘密鍵に基づいて作成した応答文字列と前記グループ参加証を送付して認証を依頼する認証依頼ステップと、前記認証者が前記グループ参加証から前記グループ固有の公開鍵に基づいて前記被認証者の公開鍵を得て、次に前記応答文字列と前記被認証者の公開鍵から前記認証用文字列に一致する文字列が得られることを確認することをもって前記被認証者が前記グループの加入者であることを認証する認証ステップと、を実行することを特徴とする。

【0021】

また、グループ認証方法の一実施形態においては、前記認証ステップの後に、前記認証者と前記被認証者が立場を入れ替えて前記グループ認証開始ステップから前記認証ステップまでを実行することを特徴とする。

【0022】

また、グループ認証方法の一実施形態においては、前記認証ステップにおける前記被認証者の認証の際に、前記グループ参加証に含まれる有効期限に関する情報に基づいて前記被認証者が前記グループの有効な加入者であるかどうかを判断することを特徴とする。

【0023】

グループ参加証更新方法の一実施形態は、グループ加入方法により前記グループ参加証を取得したメンバが前記グループ参加証の有効期限に関する情報を更新するためのグループ参加証更新方法であって、前記更新依頼者が前記管理者に対して少なくとも前記グループ参加証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する参加証更新依頼ステップと、前記管理者が前記グループ参加証から前記グループに固有の公開鍵に基づいて前記更新依頼者の公開鍵を得て、前記更新依頼者の公開鍵と新たな前記有効期限に関する情報および前記グループ固有の秘密鍵に基づいて作成した新たな前記グループ参加証を前記更新依頼者に送付する参加証更新ステップと、を実行することを特徴とする。

【0024】

また、グループ参加証更新方法の一実施形態においては、前記参加証更新依頼ステップの前に前記管理者が偽者でないことを前記更新依頼者が確認する第2の管理者確認ステップを実行することを特徴とする。

【0025】

発行者追加方法の一実施形態は、前記管理者が前記グループ参加証発行の権限を持つ発行者を追加する方法であって、発行者候補のメンバが少なくとも自分の公開鍵を前記管理者へ送付する発行者鍵送付ステップと、前記管理者が前記発行者候補の公開鍵と前記グループ固有の秘密鍵に基づいてグループ参加証発行許可証を作成し前記発行候補者に送付する参加証発行許可証発行ステップとを実行することを特徴とする。

【0026】

また、発行者追加方法の一実施形態は、前記参加証発行許可証発行ステップにおいて、前記管理者が少なくとも前記発行者候補の公開鍵、前記グループ参加証発行許可証の有効期限に関する情報および前記グループ固有の秘密鍵に基づいてグループ参加証発行許可証を作成し前記発行候補者に送付することを特徴とする。

【0027】

第2のグループ加入方法の一実施形態は、自分の公開鍵と秘密鍵を保持している加入依頼者が、前述の発行者追加方法により前記管理者からグループ参加証発行許可証の発行を受けた発行者からグループ参加証の発行を受ける第2のグループ加入方法であって、前記加入依頼者が少なくとも自分の公開鍵を送付して前記グループへの加入を依頼する第2の加入依頼ステップと、前記発行者が少なくとも前記加入依頼者の公開鍵と前記発行者の秘密鍵に基づいて作成したグループ参加証および前記発行者の前記グループ参加証発行許可証を前記加入依頼者に送付する第2の参加証発行ステップと、を実行することを特徴とする。

【0028】

また、第2のグループ加入方法の一実施形態は、前記第2の加入依頼ステップの前に前記発行者が偽者でないことを前記加入依頼者が確認する発行者確認ステップを実行することを特徴とする。

【0029】

また、第2のグループ加入方法の一実施形態は、前記第2の加入依頼ステップにおいて前記加入依頼者が前記発行者に対して自分自身を特定する情報を追加して送付し、前記発行者が前記加入依頼者を特定する情報に基づき前記加入依頼者を加入させるか否かを判断する第2の加入判断ステップを前記第2の参加証発行ステップの前に実行することを特徴とする。

【0030】

また、第2のグループ加入方法の一実施形態は、前記第2の参加証発行ステップにおいて、前記発行者が少なくとも前記加入依頼者の公開鍵、前記グループ参加証の有効期限に関する情報および前記発行者の秘密鍵に基づいて作成したグル

ープ参加証を作成し前記加入依頼者に送付することを特徴とする。

【0031】

また、第2のグループ加入方法の一実施形態は、前記第2の加入依頼ステップの前に前記グループ参加証発行許可証に含まれる有効期限に関する情報に基づいて前記発行者の前記グループ参加証発行許可証が有効かどうかを判断することを特徴とする。

【0032】

第2のグループ認証方法の一実施形態は、第2のグループ加入方法により前記グループ参加証を取得したメンバー間で前記グループへの加入資格を認証するための第2のグループ認証方法であって、認証者が被認証者に対して認証用文字列を送付する第2の認証開始ステップと、前記被認証者が前記認証者に対して少なくとも前記認証用文字列から自分の秘密鍵に基づいて作成した応答文字列と前記グループ参加証および前記グループ参加証発行許可証を送付して認証を依頼する第2の認証依頼ステップと、前記認証者が前記グループ参加証発行許可証から前記グループ固有の公開鍵に基づいて前記発行者の公開鍵を得て、次に前記グループ参加証から前記発行者の公開鍵に基づいて前記被認証者の公開鍵を得て、さらに前記応答文字列と前記被認証者の公開鍵から前記認証用文字列に一致する文字列が得られることを確認することをもって前記被認証者が前記グループの加入者であることを認証する第2の認証ステップと、を実行することを特徴とする。

【0033】

また、第2のグループ認証方法の一実施形態は、前記第2の認証ステップの後に、前記認証者と前記被認証者が立場を入れ替えて前記第2のグループ認証開始ステップから前記第2の認証ステップまでを実行することを特徴とする。

【0034】

また、第2のグループ認証方法の一実施形態は、前記第2の認証ステップにおいて前記グループ参加証に含まれる有効期限に関する情報に基づいて前記被認証者が前記グループの有効な加入者であるかどうかを判断することを特徴とする。

【0035】

また、第2のグループ認証方法の一実施形態は、前記第2の認証ステップにお

いて前記グループ参加証発行許可証に含まれる有効期限に関する情報に基づいて前記被認証者が所有する前記グループ参加証発行許可証が有効かどうかを判断することを特徴とする。

【0036】

第2のグループ参加証更新方法の一実施形態は、第2のグループ加入方法により前記グループ参加証を取得したメンバが前記グループ参加証の有効期限に関する情報を更新するための第2のグループ参加証更新方法であって、前記更新依頼者が前記発行者に対して少なくとも前記グループ参加証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する第2の参加証更新依頼ステップと、前記発行者が前記グループ参加証発行許可証から前記グループに固有の公開鍵に基づいて前記グループ参加証発行許可証を発行した発行者の公開鍵を得て、次に前記グループ参加証から前記グループ参加証発行許可証を発行した発行者の公開鍵に基づいて前記更新依頼者の公開鍵を得て、さらに前記更新依頼者の公開鍵と新たな前記有効期限に関する情報および前記発行者の秘密鍵に基づいて作成した新たな前記グループ参加証を前記更新依頼者に送付する第2の参加証更新ステップと、を実行することを特徴とする。

【0037】

また、第2のグループ参加証更新方法の一実施形態は、前記第2の参加証更新依頼ステップの前に前記発行者が偽者でないことを前記更新依頼者が確認する発行者確認ステップを実行することを特徴とする。

【0038】

発行許可証更新方法の一実施形態は、発行者追加方法により前記グループ参加証発行許可証の発行を受けた前記発行者が前記グループ参加証発行許可証の有効期限に関する情報を更新するための発行許可証更新方法であって、前記発行者が前記管理者に対して少なくとも前記グループ参加証発行許可証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する発行許可証更新依頼ステップと、前記管理者が前記グループ参加証発行許可証から前記グループに固有の公開鍵に基づいて前記発行者の公開鍵を得て、前記発行者の公開鍵と新たな前記有効期限に関する情報および前記発行者の秘密鍵に基づいて作成した新たな前記

グループ参加証発行許可証を前記発行者に送付する発行許可証更新ステップと、
を実行することを特徴とする。

【0039】

また、発行許可証更新方法の一実施形態は、前記発行許可証更新依頼ステップの前に、前記管理者が偽者でないことを前記発行者が確認する第3の管理者確認ステップを実行することを特徴とする。

【0040】

第1のグループ管理プログラムの一実施形態は、前記グループ加入方法における前記加入依頼ステップまたは前記管理者確認ステップおよび前記加入依頼ステップ、および前記グループ認証方法における前記認証依頼ステップおよび前記認証開始ステップおよび前記認証ステップ、を実行することが記述されていることを特徴とする。

【0041】

また、第1のグループ管理プログラムの一実施形態は、前記グループ参加証更新方法における前記参加証更新依頼ステップ、または前記第2の管理者確認ステップおよび前記参加証更新依頼ステップを実行することが記述されていることを特徴とする。

【0042】

第2のグループ管理プログラムの一実施形態は、前記グループ加入方法における前記参加証発行ステップまたは前記加入判断ステップおよび前記参加証発行ステップを実行することが記述されていることを特徴とする。

【0043】

また、第2のグループ管理プログラムの一実施形態は、前記グループ参加証更新方法における前記参加証更新ステップを実行することが記述されていることを特徴とする。

【0044】

第3のグループ管理プログラムの一実施形態は、前記第2のグループ加入方法における前記第2の加入依頼ステップまたは前記発行者確認ステップおよび前記第2の加入依頼ステップ、および前記第2のグループ認証方法における前記第2

の認証依頼ステップおよび前記第2の認証開始ステップおよび前記第2の認証ステップを実行することが記述されていることを特徴とする。

【0045】

また、第3のグループ管理プログラムの一実施形態は、前記第2のグループ参加証更新方法における第2の参加証更新依頼ステップを実行することが記述されていることを特徴とする。

【0046】

また、第3のグループ管理プログラムの一実施形態は、前記第2のグループ参加証更新方法における前記発行者確認ステップを実行することを特徴とする。

【0047】

第4のグループ管理プログラムの一実施形態は、前記発行者追加方法における前記発行者鍵送付ステップ、および前記第2のグループ加入方法における前記第2の参加証発行ステップ、および実行することが記述されていることを特徴とする。

【0048】

また、第4のグループ管理プログラムの一実施形態は、前記発行許可証更新方法における前記発行許可証更新依頼ステップを実行することが記述されていることを特徴とする。

【0049】

また、第4のグループ管理プログラムの一実施形態は、前記発行許可証更新方法における前記第3の管理者確認ステップを実行することが記述されていることを特徴とする。

【0050】

第5のグループ管理プログラムの一実施形態は、前記発行者追加方法における前記参加証発行許可証発行ステップ、および前記発行許可証更新方法における前記発行許可証更新ステップを実行することが記述されていることを特徴とする。

【0051】

グループ管理プログラムを記録する記録媒体の一実施形態は、前記第1から第5のグループ管理プログラムの一部または全部が記録されていることを特徴とす

る。

【0052】

第1のグループ管理システムの一実施形態は、少なくとも前記第1のグループ管理プログラムを実行可能な状態で保持する第1の端末と、少なくとも前記第2のグループ管理プログラムを実行可能な状態で保持する第2の端末と、から少なくとも構成されることを特徴とする。

【0053】

第2のグループ管理システムの一実施形態は、少なくとも前記第3のグループ管理プログラムを実行可能な状態で保持する第3の端末と、少なくとも前記第4のグループ管理プログラムを実行可能な状態で保持する第4の端末と、少なくとも前記第5のグループ管理プログラムを実行可能な状態で保持する第5の端末と、から少なくとも構成されることを特徴とする。

【0054】

本願発明は、以下の記載の「発明の実施の形態」および添付の図面を用いて説明されるが、これは例示を目的とするものであって、本願発明は、これらに限定されるものではない。

【0055】

【発明の実施の形態】

まず、本発明の実施形態の構成について概要を説明する。本発明はネットワークで互いに接続された複数の機器間の通信方法に関するものである。

【0056】

本発明はイーサネット、アナログまたはデジタルの公衆回線または専用回線を用いたネットワーク、ADSL (Asymmetric Digital Subscriber Line)、無線LAN (Local Area Network) などの物理的なネットワークを想定しているが、これらに制限されるものではない。また、インターネットではネットワークの下位プロトコルとしてTCP/IP (Transmission Control Protocol/Internet Protocol) が広く使用されており本発明もその使用を想定しているが、これに制限されるものでもない。

【0057】

前記機器のそれぞれに前記物理的なネットワークに対応した通信インタフェースが備わっており、前記通信インタフェースを制御して通信を行うためのプログラムを前記機器内のCPUが実行することにより通信処理が行われる。前記プログラムは前記機器のROM (Read Only Memory) に記録されている場合、あるいは前記機器のハードディスクやリムーバブルディスクなど不揮発記憶装置に格納されていてそこから必要に応じて前記機器のRAM (Random Access Memory) に読み込まれて実行される場合、あるいはこれらを組み合わせて実行する場合などがある。

【0058】

また前記機器には機器使用者の入力を受け付けるための入力手段も備わっている。入力手段としては通常キーボード、マウス、タブレットなどが用いられる。これらの構成についてはパーソナルコンピュータなどで一般的に知られているものであり、本発明の主眼ではないので詳細な説明は省略する。

【0059】

なお、以下で用いる「ユーザ」という用語は、前記機器、前記機器で動作するプログラムおよび機器使用者を含む概念である。本発明が想定しているネットワークにおいては、各ユーザは、必ずしも常時ネットワークに接続しているわけではなく、通信に必要な各ユーザのアドレス情報 (IPアドレス、ポート番号など) も固定ではなくネットワークに接続するたびに变化する可能性がある。

【0060】

(実施の形態1)

本発明の第一の実施の形態について説明する。

【0061】

まず、本実施の形態で用いている公開鍵暗号化方式の概要を説明する。公開鍵暗号化方式とは、次のような数学的性質を持つ二つの暗号鍵、「公開鍵」と「秘密鍵」を用いた暗号化方式である。(1) 公開鍵と秘密鍵は、一方から現実的な時間で他方を計算することが互いに不可能である。(2) 公開鍵で暗号化した情報は対応する秘密鍵でのみ復号可能であり、逆もまた成立する。

【0062】

上記(1)の性質により、利用者は秘密鍵のみを秘密裡に保持しておけば、公開鍵を第三者に知られても問題ないので公開鍵を公開しておくことができる。従って、情報を秘密裡に送信したい送信者は、前もって受信者の公開鍵を入手しておき情報を受信者の公開鍵で暗号化したものを送信する。受信者は自分のみが持つ秘密鍵でそれを復号することができ、暗号化前の情報を得ることができる。第三者が暗号化された情報を傍受しても、受信者の秘密鍵でしか復号できないため情報が漏洩することはない。以下では、暗号化対象の情報Mを鍵Kで暗号化したものを $e(M, K)$ のように表記することとする。

【0063】

また、公開鍵暗号化方式を用いて、情報そのものは暗号化しないが、情報が改ざんされていないことを証明するための電子「署名」を行うことも可能である。すなわち、署名対象の情報Mから所定のアルゴリズム f で一意に導き出される派生情報 $H = f(M)$ を送信者の秘密鍵KSで暗号化した $Sgn = e(H, KS)$ を署名情報として元の情報Mに付加して送信する。受信者は、Mと Sgn を受信し、 Sgn を送信者の公開鍵KPで復号化してHを得て、 $H = f(M)$ が成立することを確認することで情報Mが第三者によって改ざんされていないことを確認できる。なぜならばMが第三者により改ざんされていれば $H = f(M)$ が成立せず、また送信者の秘密鍵KSがなければ、送信者の公開鍵KPで正常に復号できる Sgn の作成も不可能だからである。

【0064】

公開鍵暗号化方式およびこれに応用した署名方式は、インターネットでセキュリティを要する通信に広く用いられている。以下では、あるユーザAの公開鍵、秘密鍵をそれぞれ KA_P 、 KA_S のように表記する。

【0065】

本願においてグループは次のように定義する。(1)グループは一名以上のネットワーク参加者からなる(2)ユーザは複数のグループに属することが可能である(3)グループにはグループ固有の共有情報がある(4)同じグループに属することを互いに認証されたメンバ間ではそのグループの共有情報の送受信を

行うことができる。グループを構成するメンバは、友人、家族、同じ趣味の持ち主、住所が近い者、の集合などが考えられる。

【0066】

本実施の形態においては、グループを構成するメンバをグループ参加証を発行する権限をもつ管理者および一般ユーザに分類する。一般ユーザにグループ参加証を発行できるのは管理者のみであり、ユーザはグループ参加証を管理者に発行してもらうことでグループへの参加が可能となる。本願において、グループ参加証とは、あるグループのメンバが、他のグループメンバに対して、当該グループに参加していることを証明するための情報であると定義される。

【0067】

このようなグループを管理するには、以下に示すような処理が必要となる。

【0068】

- (1) グループの生成
- (2) グループの告知
- (3) グループの発見
- (4) グループ管理者の特定
- (5) グループへの新規加入依頼
- (6) グループメンバ間の認証
- (7) グループメンバ間の情報共有
- (8) グループ参加証の更新
- (9) グループメンバの削除
- (10) グループ管理者の追加
- (11) グループ公開鍵の更新

以下、各処理について説明する。

【0069】

1. グループの生成

情報共有のためにグループを作成したいユーザAは、そのグループ用の公開鍵KG_Pおよび秘密鍵KG_Sのペアを作成する。これらはAが指定した情報（パスフレーズ）を元に生成されたものであってもよいし、プログラムまたは装置

が生成した乱数などの情報を元に生成されたものであってもよい。

【 0 0 7 0 】

2. グループの告知

生成したグループ公開鍵 KG_P は、そのグループを特定する情報、例えば望ましくは他のグループと重複しないグループ ID と共に何らかの方法でグループ情報として告知される。この告知方法としては、(1) 従来の技術の説明に用いた図 15 にて例示したような P2P ネットワークの全てあるいは一部のユーザを宛て先として A がグループ情報を発信し、そのグループ情報が図 15 の検索情報の流れのようにユーザからユーザへと順次転送され、最終的に宛て先とされたユーザが受信することで実現してもよいし、(2) 物理的に A と同じローカルエリアネットワーク (LAN) または仮想プライベートネットワーク (VPN) に属している他のユーザ宛てにグループ情報をブロードキャストすることで実現してもよいし、あるいは、(3) A が電子メール、郵便等を含む、P2P ネットワークを介した転送以外の何らかの方法で他のユーザに対して少なくともグループ公開鍵 KG_P を直接送信することで実現してもよいし、さらには、(4) グループ情報のリストを保持し検索の用途に供するグループ情報インデックスサーバを運営し、前記グループ情報をこのグループ情報インデックスサーバに登録することによって実現してもよいし、(5) これらを複数組み合わせることで実現することも可能である。

【 0 0 7 1 】

なお、前記グループ情報には、そのグループ名、グループの生成者を特定する情報、成り立ち、目的、参加条件等、当該グループの内容を説明する情報と共に告知されていても構わないし、グループ公開鍵 KG_P のみをグループ情報として告知しても構わない。

【 0 0 7 2 】

3. グループの発見

P2P ネットワークに参加しているユーザ X は、次のいずれかの方法でグループを発見し、グループを特定する情報、少なくともグループ公開鍵 KG_P を入手する。(1) X が保持している、過去に告知され受信したグループ情報 (グル

ープを生成したAから直接受け取ったグループ情報を含む)から、グループを特定する情報あるいはグループを説明する情報に基づき所望のグループを発見する。(2)図15に例示したようなP2Pネットワークの情報検索の仕組みを用いて他のユーザに対してグループを特定する情報あるいはグループを説明する情報の一部または全部をキーとして検索し、該当するグループ情報を保持しているユーザからグループ情報を入手する。(3)前記グループ情報インデックスサーバが運用されている場合には、このグループ情報インデックスサーバに対してグループを特定する情報あるいはグループを説明する情報の一部または全部をキーとして検索し、所望のグループのグループ情報を入手する。(4)グループを生成したAがXにとって既知の場合は、グループ情報をAから何らかの手段で直接入手する。

【0073】

4. グループ管理者の特定

グループ管理者とは、グループメンバの追加削除の権限を持つユーザであり、より具体的にはグループ秘密鍵KG_Sを保持するユーザである。あるグループへ新規加入したいユーザXは、5.で説明するようにグループ管理者Aと直接通信する必要があり、そのために必要なグループ管理者Aのアドレス情報、例えばIPアドレス、通信に用いるポート番号、などを特定する必要がある。それは例えば次のいずれかの方法で行われる。(1)Xは図15に例示したようなP2Pネットワークの情報検索の仕組みを用いてグループを特定する情報の一部または全部をキーとして検索を行い、この検索要求を受けた該当するグループの管理者がこれに応答し、自分のアドレス情報をXに対して通知する。(2)ピア情報サーバを用いる方法である。ピア情報サーバとは、現在オンライン状態である全ユーザ、あるいは少なくとも一つのグループの管理者である全ユーザの、少なくともアドレス情報および当該ユーザが管理者であるグループのグループを特定する情報を収集して検索の用途に供するサーバである。Xはこのピア情報サーバに対してグループを特定する情報をキーとして検索を行い、その検索結果として管理者のアドレス情報を入手する。(3)グループ管理者AがXにとって既知であり、かつグループ管理者Aが常にオンラインであってアドレス情報が変化しないこ

とも既知である場合、そのアドレス情報を用いる。

【0074】

5. グループへの新規加入依頼

あるグループへ新規加入したいユーザXは、前記4. で特定したアドレス情報を用いてグループ管理者Aと通信を行い、6. で必要となるグループ参加証の発行を依頼する。本処理の詳細については後述する。

【0075】

6. グループメンバー間の認証

前記5. で入手したグループ参加証を持つグループメンバー間では、互いに同じグループに属していることを認証することが可能になる。本処理の詳細については後述する。

【0076】

7. グループメンバー間の情報共有

前記6. で互いに同じグループに属していると認証された複数のグループメンバー間、例えばXとYの間ではグループの共有情報の相互の転送が可能になる。これは、例えば次のようなステップを順に実行することにより行われる。

【0077】

(7-1) 通信に用いる暗号鍵の設定

前記6. で互いに同じグループに属していることを認証した後、暗号鍵K_XYを一方、例えばX、が作成して、Xの秘密鍵およびYの公開鍵でこの暗号鍵を暗号化してYに送付する。Yはこれを自分の秘密鍵およびXの公開鍵を用いて復号可能であり、またY以外はこれを復号することができない。これにより、安全にK_XYをXからYに通知する。

【0078】

(7-2) 情報転送の暗号化

以降のXとYの間の情報転送は、共通鍵K_YXで暗号化して行う。第三者はK_XYを知ることができないので、XY間の通信を傍受してもその内容を復号することはできず、またXまたはYに成りすまして偽の情報をYまたはXに転送することも不可能となり、XとYは安全に情報転送を行うことができる。これに

より、グループメンバ相互間での安全なグループ情報の共有が可能となる。

【0079】

なお、3名以上のメンバがお互いに認証された状態である場合、このメンバ間の情報転送に用いる暗号鍵には次のような選択肢がある。

【0080】

(1) 異なる二者間の通信には異なる暗号鍵を用いる。例えば、AとBとCが互いに認証されている場合、AとBの間の通信には暗号鍵K_ABを、BC間はK_BC、CA間はK_CAを用いる方法である。

【0081】

(2) 互いに認証された複数メンバ間で共通の暗号鍵を用いる。例えば、AとBが互いに認証されていて暗号鍵K_ABを用いて通信している状態でCが新たにAまたはBとの認証処理を行って認証された場合、AまたはBからCへCの公開鍵を用いて安全にK_ABを送付し、以降はA、B、Cのいずれの二者間でも暗号鍵K_ABを用いる方法である。

【0082】

8. グループ参加証の更新

前記5. で発行されるグループ参加証に有効期限情報が含まれている場合には、当該有効期限以降、グループへの参加（グループメンバ間の認証）が不可能になるため、ユーザはグループ参加証の更新が必要となる。本処理の詳細については後述する。

【0083】

9. グループメンバの削除

上記で述べてきた方法では、グループ参加証を持つユーザは、そのグループ参加証の有効期限まではグループへの参加が可能であるが、何らかの理由により、その有効期限以前にそのユーザをグループメンバから除外したい（そのユーザをグループメンバとして認証できないようにしたい）場合は、例えば次のような処理を実行することで可能となる。グループメンバの削除について、グループ参加証の消去（下記（9-1））および失効者情報の作成（下記（9-2-1）～（9-2-4））の2例を挙げて説明する。

【0084】

(9-1) グループ参加証の消去

除外対象メンバが保持しているグループ参加証を消去すれば、当該メンバはその後前記6. で述べたグループメンバ間の認証が行えなくなる。そのためには次のような処理を実行する必要がある。

【0085】

(9-1-1) グループ参加証の消去指示

グループ管理者がメンバを除外することを指定することを指示する参加証消去指示ステップを実行する。

【0086】

(9-1-2) グループ参加証の消去

上記参加証消去指示を受けた当該メンバは、自分が保持しているグループ参加証を消去する。これは機器の使用者が手動で消去する方法でも良いが、この場合は指示を無視して故意に消去しない場合も考えられるので、上記参加証消去指示を受けた機器あるいはプログラムが強制的に消去する方法でもよい。

【0087】

(9-2-1) 失効者情報の作成

グループメンバの一人（グループ管理者含む）が、除外されたメンバを特定する情報、例えば当該メンバの公開鍵、を含む失効者情報を作成する。

【0088】

(9-2-2) 失効者リストの共有前記6. のグループメンバ間の認証の際には、自分が保持する失効者情報のリストと認証相手が持つ失効者情報のリストを比較し、一方が保持しない失効者情報が存在する場合は互いに他方の失効者リストに追加することで、失効者情報のリストを全グループメンバで共有するようにする。

【0089】

(9-2-3) 失効者の除外

前記6. のグループメンバ間の認証の際に、認証相手が自分の保持する失効者リストに含まれているかどうかを確認し、含まれている場合は相手をグループメ

ンバであると認証しない。例えばユーザの公開鍵を失効者情報として用いる場合は、認証相手の公開鍵がリストに含まれる失効者情報のいずれかと一致すれば、この相手の認証を拒否する。

【0090】

(9-2-4) 失効者の参加資格更新の拒否

前記8.においてグループ参加証の更新を行う際に、参加証の更新を依頼したユーザがリストに含まれる失効者情報のいずれかと一致するかどうかを確認し、一致するものがある場合は参加証の更新を拒否する。

【0091】

なお、失効者情報にその消去期限を含めておいて、消去期限を越えた失効者情報を削除することが可能である。例えば、グループ参加証の有効期限より少し後の時点を消去期限として付与しておけば、不要となった失効者情報を順次削除することができ、失効者情報のリストが無限に増大することを防ぐことができる。

【0092】

また、失効者情報の作成はグループ管理者のみが行い、グループ管理者がグループ秘密鍵KG_Sを用いて暗号化した状態で共有することとしてもよい。グループメンバは公開されているグループ公開鍵KG_Pを用いて失効者情報を復号することが可能であり、この失効者情報が不正に改ざんされていないことの確認が可能となる。これにより、悪意を持つユーザにより作成された不正な失効者情報が共有されることを防ぐことができる。

【0093】

また、グループ参加証の消去(上記(9-1))の方法と、失効者情報の作成(上記(9-2-1)～(9-2-4))による方法とを、必要に応じて組み合わせることによって、目的のメンバを削除してもよい。

【0094】

10. グループ管理者の追加

前記5.で述べたグループへの新規加入は、グループ管理者がオンラインである場合にしか行えない。グループ生成直後はグループを生成したユーザー一人のみがグループ管理者であるが、グループへの新規加入の機会を増やすために、グル

ープ管理者を増やすことが可能である。これは、グループ秘密鍵KG__Sを何らかの安全な手段、すなわち暗号化通信または郵送などの手段によってグループ管理者から別のユーザ（追加されるべき別のグループ管理者）に転送することによって実現することができる。

【0095】

11. グループ公開鍵の更新

何らかの事故によりグループ秘密鍵KG__Sがグループ管理者以外のユーザに漏洩した場合、グループ秘密鍵を入手したユーザは不正にグループ参加証または失効者リストを発行することが可能となり、かつグループメンバには本来のグループ管理者が発行したグループ参加証と不正に発行されたグループ参加証を判別することはできない。このような場合には、グループ公開鍵・秘密鍵のペアを更新する以外に不正を防ぐ方法はない。また、前記10.で追加されたグループ管理者のいずれかからユーザ追加削除の権限を剥奪したい場合も、グループ公開鍵・秘密鍵のペアを更新する以外の方法はない。一方、グループ管理者がグループ公開鍵・秘密鍵をそれぞれKG__P'、KG__S'に更新したとしても、従来のグループ公開鍵KG__Pとそれに基づいて作成されたグループ参加証を持つグループメンバ同士では前記6.のグループ認証は互いに可能なままなので、グループメンバは常に最新のグループ公開鍵を保持しておく必要があると同時に、最新のグループ公開鍵に対応したグループ参加証を入手する必要がある。

【0096】

最新のグループ公開鍵の保持は、例えば次のいずれかのような方法により可能である。

【0097】

(1) グループ管理者がグループ公開鍵・秘密鍵を更新した時点で、図15に例示したようなP2Pネットワークを介してネットワーク参加者全員に新しいグループ公開鍵を送付する。対応するグループのメンバは、この新しいグループ公開鍵で自分が保持しているグループ公開鍵を置き換える。

【0098】

(2) 前記2.で告知されるグループ情報に、グループ公開鍵の更新時刻に関

する情報も含めておき、前記各グループメンバはグループ公開鍵に加えてこのグループ公開鍵の更新時刻に関する情報も保持しておく。そして、前記6.のグループ認証時には双方が持つグループ公開鍵とその更新時刻の比較を行い、新しい方のグループ公開鍵で古いほうのグループ公開鍵を置き換える。

【0099】

(3) 前記2.の(4)におけるグループ情報インデックスサーバを運営している場合には、グループ情報に(1)同様グループ公開鍵の更新時刻に関する情報も含めておき、グループメンバはオンラインになった時、一定時間おき、あるいは前記6.のグループ認証を行う直前、などのタイミングで前記グループ情報インデックスサーバにアクセスして当該グループの最新のグループ公開鍵を入手する。

【0100】

最新のグループ公開鍵に対応したグループ参加証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼(前記8.)を実行すればよい。

【0101】

次に、前記5.で概要を述べたグループへの新規加入依頼の処理の流れについて、図1と図2を参照して順を追って詳細に説明する。図1はグループへの新規加入を依頼する加入依頼者Xとグループ管理者Aでそれぞれ実行される処理の流れを図示したものである。図2はグループへの新規加入が実行された後、加入依頼者Xが保持している情報を表している。

【0102】

[ステップ101]

事前に、グループ管理者Aはグループの公開鍵KG_P・秘密鍵KG_Sのペアを作成し、このうちグループ公開鍵KG_Pについては公開しておく(前記1.および前記2.を参照)。

【0103】

[ステップ102]

同じく事前に、加入依頼者Xは自分の公開鍵KX_P・秘密鍵KX_Sのペア

を作成しておく。これはXが指定した情報（パスフレーズ）を元に生成されたものであってもよいし、プログラムまたは装置が生成した乱数に基づいて生成されたものであってもよい。

【0104】

[ステップ103]

Xは参加を所望するグループの公開鍵 KG_P を入手し（前記3. 参照）、またグループの管理者Aを特定する（前記4. 参照）。

【0105】

[ステップ104]

Xは任意の文字列Sを作成する。これはXが入力した文字列そのものであってもよいし、プログラムまたは装置が生成した乱数に基づく文字列であってもよい。

【0106】

[ステップ105]

XはAに文字列Sと自分を特定できる情報、例えば名前、住所、などを送付してグループへの新規加入を依頼する。

【0107】

[ステップ106]

AはXから送られたXを特定する情報に基づき、Xの加入を承認するか否かを決定する。加入を否認した場合は、Xがグループへ新規加入できないまま処理は終了する。

【0108】

[ステップ107]

AはXから送られた文字列Sをグループの秘密鍵 KG_S で暗号化した文字列 $S' = e(S, KG_S)$ を作成し、Xに送信する。

【0109】

[ステップ108]

XはAから受信した S' をグループ公開鍵 KG_P で復号する。

【0110】

【ステップ109】

XはS'がKG_Pにより正常に復号され、かつその結果が元の文字列Sに等しいことを確認する。これにより、S'がグループ公開鍵KG_Pに対応する秘密鍵KG_Sによって暗号化されたこと、すなわちAが確かにグループ秘密鍵KG_Sを保持するグループ管理者であることが確認できる。復号が失敗あるいは復号結果がSに等しくない場合はAがグループ管理者であることが確認できないのでXがグループへ新規加入できないまま処理は終了する。

【0111】

【ステップ110】

XはAに自分の公開鍵KX_Pを送信する。

【0112】

【ステップ111】

AはXのグループ参加証を作成し、Xに送付する。グループ参加証は、Xの公開鍵KX_Pに参加証の効果が消滅する日時T_Xを添付したもの（以下“+”で表記）をグループ秘密鍵KG_Sで暗号化して作成したものであり、

$$C_X = e(KX_P + T_X, KG_S)$$

と表せる。KX_PへのT_Xの添付方法は、両者がまとめて暗号化されていて復号前には分離不可能であり、一方復号時にはそれぞれを分離することが可能であればどのような方法であってもよい。例えばKX_P、T_Xをそれぞれ文字列表現したものを所定の分離文字を介して文字列結合したものなどが考えられる。

【0113】

【ステップ112】

Xはグループ参加証C_Xを受け取り、グループへの新規加入処理が完了する。グループへの新規加入が完了した時点でXが保持する情報は図2に示す通りである。

【0114】

なお、本実施の形態では前記ステップ105においてXが自分を特定できる情報を、前記ステップ110の時点でXの公開鍵を、それぞれAに対して送信する

こととしているが、これら情報は前記ステップ105、前記ステップ110のいずれであってもよいしその順序も特に限定されない。

【0115】

次に、前記6.で概要を説明した、参加証を獲得したXが他のグループメンバに同じグループに属していることを認証してもらう処理の流れについて、図3を参照して順を追って詳細に説明する。図3はグループ参加証を既に入手した二人のグループ参加者Xとグループ参加者Yでそれぞれ実行される処理の流れを図示したものである。なお、Xは図2に示した内容の各種鍵、参加証を既に保持しているものとする。

【0116】

[ステップ301]

Xはグループに属している他のメンバYのアドレス情報を特定する。それは例えば次のいずれかの方法で行われる。(1) Xは図15に例示したようなP2Pネットワークの情報検索の仕組みを用いてグループを特定する情報の一部または全部をキーとして検索を行い、該当するグループに属しているユーザがこれに回答し、自分のアドレス情報をXに対して通知する。(2) 現在オンライン状態である全ユーザの少なくともアドレス情報および当該ユーザが属するグループのグループを特定する情報を収集して検索の用途に供するピア情報サーバが運営されている場合、Xはこのピア情報サーバに対してグループを特定する情報をキーとして検索を行い、その検索結果としてオンラインである他のグループメンバのアドレス情報を入手する。(3) 他のグループメンバYがXにとって既知であり、かつYが常にオンラインであってアドレス情報が変化しないことも既知である場合、そのアドレス情報を用いる。

【0117】

[ステップ302]

XはYに対し認証を依頼する。

【0118】

[ステップ303]

Yは、前記ステップ104同様、任意文字列Sを作成しXに送信する。

【0119】

[ステップ304]

XはSを自分の秘密鍵 KX_S で暗号化した文字列 $S' = e(S, KX_S)$ を作成し、 S' と自分の保持しているグループ参加証 C_X をYに送信する。

【0120】

[ステップ305]

YはXから送られた参加証 C_X をグループ公開鍵 KG_P で復号し、 K_X 、 P と T_X を得る。

【0121】

[ステップ306]

Yは前記ステップ305において復号が成功したことを確認する。もし失敗した場合は、参加証 C_X が正しくグループ秘密鍵 KG_S で暗号化されていないことを意味するので、Xはグループに属していないとみなされ処理は終了する。

【0122】

[ステップ307]

Yは前記ステップ305で得られた有効期限 T_X が過ぎていないことを確認する。もし過ぎていれば参加証が無効であることを意味するので、Xはグループに属していないとみなされ処理は終了する。

【0123】

[ステップ308]

YはXから送られた S' を前記ステップ305で得られたXの公開鍵 KX_P で復号する。

【0124】

[ステップ309]

Yは前記ステップ308の復号が成功し、かつ復号結果がSと一致することを確認する。一致しなければ、Xは公開鍵 KX_P に対応する秘密鍵 KX_S を持っていないことを意味するので、Xは第三者の成りすましの可能性があるとしてみなされ処理は終了する。

【0125】

【ステップ310】

Yは以下のことが全て確認できたので、Xをグループ参加者であると認証する。
 (1) グループ管理者がグループ秘密鍵KG_Sで暗号化したグループ参加証を保持している。
 (2) グループ参加証の有効期限は切れていない。
 (3) Xはグループ参加証に暗号化されていた公開鍵KX_Pに対応する秘密鍵KX_Sを保持している。

【0126】

次に、前記ステップ302から前記ステップ310までを、XとYの立場を入れ替えて実行する。この処理が成功すれば、XはYをグループ参加者であると認定し、相互の認定が完了する。

【0127】

次に、前記8.で概要を説明した、グループ参加証を更新する処理の流れについて、図4を参照して順を追って詳細に説明する。図4はグループ参加証の更新を依頼する更新依頼者Xとグループ管理者Aでそれぞれ実行される処理の流れを図示したものである。なお、Xは図2に示した内容の各種鍵、参加証を既に保持しているものとする。

【0128】

【ステップ401】

グループ参加証を更新したいユーザXは、グループ管理者Aのアドレス情報を特定する(前記4.を参照)。

【0129】

【ステップ402】

Xは任意の文字列Sを作成し、Aへ送信してグループ参加証の更新を依頼する。この文字列はXが入力した文字列そのものであってもよいし、プログラムまたは装置が生成した乱数に基づく文字列であってもよい。

【0130】

【ステップ403】

グループ管理者AはSをグループ秘密鍵KG_Sで暗号化した文字列 $S' = e(S, KG_S)$ を作成しXへ送信する。

【0131】

[ステップ404]

XはS' をグループ公開鍵KG__Pにより復号する。

【0132】

[ステップ405]

XはS' がグループ公開鍵KG__Pにより正常に復号され、かつその結果が元の文字列Sに等しいことを確認する。これにより、S' がグループ公開鍵KG__Pに対応する秘密鍵KG__Sによって暗号化されたこと、すなわちAが確かにグループ秘密鍵KG__Sを保持するグループ管理者であることが確認できる。復号が失敗あるいは復号結果がSに等しくない場合はAがグループ管理者であることが確認できないのでXはグループ参加証を更新することなく処理は終了する。

【0133】

[ステップ406]

XはAへ自分の参加証 $C_X = e(KX_P + T_X, KG_S)$ を送信する。

【0134】

[ステップ407]

Aは受信した C_X をグループ公開鍵KG__Pで復号して KX_P を得る。

【0135】

[ステップ408]

Aは前記ステップ407での復号が成功したことを確認する。復号に失敗した場合は、Xがグループ秘密鍵KG__Sで暗号化されたグループ参加証を持たない、すなわちXはグループメンバーではないとみなしてXのグループ参加証を更新することなく終了する。

【0136】

[ステップ409]

AはXの公開鍵 KX_P に新たな有効期限 T_X' を添付したものをグループ秘密鍵KG__Sで暗号化して新たな参加証 $C_X' = e(KX_P + T_X', KG_S)$ を作成してXに送信する。

【0137】

[ステップ410]

Xは新しい参加証C_X'を受信する。

【0138】

この処理により、Xの参加証には新たな有効期限が添付されるのでXはその新たな有効期限までグループに参加することができるようになる。

【0139】

このように、本第一の実施の形態によれば、グループ管理者が介在しなくても（オフラインであっても）、グループ管理者にグループ参加証を発行されたグループメンバ同士で互いにグループメンバであることの認証が可能となる。

【0140】

また、仮にグループからあるユーザを除外したい事態が発生しても、グループ参加証が有効期限を含んでいることにより、少なくともその有効期限後はそのユーザがグループメンバとして認証されないようにすることが可能となる。さらにその有効期限までの間は失効リストを参照してそのユーザをグループ認証から除外することが可能である。

【0141】

（実施の形態2）

前述した第一の実施の形態では、グループを構成するメンバとしては管理者と一般ユーザだけとしているが、第一の実施の形態の10.で述べたように、グループメンバの新規加入機会を増やすためには管理者を増やす、すなわちグループ秘密鍵を複製することが必要であるが、グループ秘密鍵が複数のユーザに保持されることで、漏洩する可能性が高くなるという課題がある。

【0142】

本実施の形態はこれを改善するものであり、グループを構成するメンバを唯一の管理者、グループ参加証発行許可証を保持し、グループ参加証を発行する権限を持つ発行者、および一般ユーザに分類する。発行者に権限を与えることができるのは管理者のみであり、一般ユーザにグループ参加証を発行できるのは管理者および発行者である。

【0143】

こうすることにより、管理者が複数の発行者を設けておけば、グループの秘密鍵を複製することなくユーザの新規加入機会を増やすことが可能となる。

【0144】

このようなグループを管理するには、以下に示すような処理が必要となる。

【0145】

- (1) グループの生成
- (2) グループの告知
- (3) グループ発行者の追加
- (4) グループの発見
- (5) グループ発行者の特定
- (6) グループへの新規加入依頼
- (7) グループメンバー間の認証
- (8) グループメンバー間の情報共有
- (9) グループ参加証の更新
- (10) グループ参加証発行許可証の更新
- (11) グループメンバーの削除
- (12) グループ公開鍵の更新

以下、各処理について説明する。ただし第一の実施の形態と同一のものについてはその旨記して説明を省略している。

【0146】

1. グループの生成

第一の実施の形態の1. グループの生成と同じであるので省略する。

【0147】

2. グループの告知

第一の実施の形態の2. グループの告知と同じであるので省略する。

【0148】

3. グループ発行者の追加

前記1. でグループを生成したユーザ（グループ管理者）は、グループ参加証

発行許可証を発行することでグループメンバを追加する権限を持つユーザを必要人数追加することができる。すなわち、グループ参加証発行許可証を発行されたユーザは他のユーザに対してグループ参加証を発行することが可能となる。グループ管理者がグループ参加発行許可証を発行したユーザをグループ発行者と呼ぶ。本処理の詳細については後述する。

【0149】

4. グループの発見

第一の実施の形態の3. グループの発見と同じであるので省略する。

【0150】

5. グループ発行者の特定

あるグループへ新規加入したいユーザXは、6. で説明するようにグループ発行者と通信する必要がある、そのために必要なグループ発行者のアドレス情報を特定する必要がある。それは例えば次のいずれかの方法で行われる。(1) Xは図15に例示したようなP2Pネットワークの情報検索の仕組みを用いてグループを特定する情報の一部または全部をキーとして検索を行い、この検索要求を受けた該当するグループのグループ発行者がこれに応答し、自分のアドレス情報をXに対して通知する。(2) 現在オンライン状態である全ユーザ、あるいは少なくとも一つのグループの管理者または発行者である全ユーザの、少なくともアドレス情報および当該ユーザが管理者または発行者であるグループのグループを特定する情報を収集して検索の用途に供するピア情報サーバが運営されている場合、Xはこのピア情報サーバに対してグループを特定する情報をキーとして検索を行い、その検索結果として発行者のアドレス情報を入手する。(3) グループ発行者がXにとって既知であり、かつ当該グループ発行者が常にオンラインであってアドレス情報に変化しないことも既知である場合、そのアドレス情報を用いる。

【0151】

6. グループへの新規加入依頼

グループへ新規加入したいユーザXは、前記5. で特定したアドレス情報を用いてグループ発行者と通信を行い、7. で必要となるグループ参加証の発行を依

頼する。本処理の詳細については後述する。

【0152】

7. グループメンバー間の認証

前記6. で入手したグループ参加証を持つグループメンバー間では、互いに同じグループに属していることを認証することが可能になる。本処理の詳細については後述する。

【0153】

8. グループメンバー間の情報共有

第一の実施の形態の前記7. と同じであるので省略する。

【0154】

9. グループ参加証の更新

前記6. で発行されるグループ参加証に有効期限情報が含まれている場合には、当該有効期限以降、グループへの参加（グループメンバー間の認証）が不可能になるため、ユーザはグループ参加証の更新が必要となる。本処理の詳細については後述する。

【0155】

10. グループ参加証発行許可証の更新

前記3. で発行されたグループ参加証発行許可証に有効期限情報が含まれている場合には、当該有効期限以降グループ参加証の発行が不可能になるため、発行者はグループ参加証発行許可証の更新が必要となる。本処理の詳細については後述する。

【0156】

11. グループメンバーの削除

第一の実施の形態同様、何らかの理由により、グループ参加証の有効期限以前に特定のメンバーをグループメンバーから除外したい場合がありえる。

【0157】

当該メンバーのグループ参加証を消去する方法は、第一の実施の形態の前記9. における方法において「グループ管理者」を「グループ管理者またはグループ発行者」に置き換えた場合と同一であるので詳細な説明は省略する。第一の実施の

形態同様、失効者情報を作成・共有する方法をとることも可能である。すなわち、例えば次のような処理を実行する。

【0158】

(11-1) 失効者情報の作成

グループメンバの一人（グループ管理者、グループ発行者含む）が、除外されたメンバを特定する情報、例えば当該メンバの公開鍵、を含む失効者情報を作成する。

【0159】

(11-2) 失効者リストの共有

前記7. のグループメンバ間の認証の際には、自分が保持する失効者情報のリストと認証相手が持つ失効者情報のリストを比較し、一方のリストに含まれない失効者情報が存在する場合は互いに他方のリストに追加することで、失効者情報のリストを全グループメンバで共有するようにする。

【0160】

(11-3) 失効者の除外

前記7. のグループメンバ間の認証の際に、認証相手が自分の保持する失効者情報のリストに含まれているかどうかを確認し、含まれている場合は相手をグループメンバであると認証しない。例えばユーザの公開鍵を失効者情報として用いる場合は、認証相手の公開鍵がリストに含まれる失効者情報のいずれかと一致すれば、この相手の認証を拒否する。

【0161】

(11-4) 失効者の参加資格更新の拒否

前記9. においてグループ参加証の更新を行う際に、参加証の更新を依頼したユーザがリストに含まれる失効者情報のいずれかと一致するかどうかを確認し、一致するものがある場合は参加証の更新を拒否する。

【0162】

なお、失効ユーザ情報にその消去期限を含めておいて、消去期限を越えた失効者情報を削除することが可能であるのは第一の実施の形態同様である。

【0163】

また、第一の実施の形態同様、失効者情報の作成はグループ発行者のみが行い、グループ発行者が自分の秘密鍵を用いて暗号化した状態で共有することとしてもよい。グループメンバは失効者情報とそれを発行したグループ発行者の参加証発行許可証を同時に入手することにより、この参加証発行許可証に含まれるグループ発行者の公開鍵を用いて失効者情報を復号することが可能であり、この失効者情報が不正に改ざんされていないことの確認が可能となる。これにより、悪意を持つユーザにより作成された不正な失効者情報が共有されることを防ぐことができる。

【 0 1 6 4 】

1 2. グループ公開鍵の更新

何らかの事故によりグループ秘密鍵KG__Sがグループ管理者以外のユーザに漏洩した場合、グループ秘密鍵を入手したユーザは不正にグループ参加証発行許可証を発行することが可能となり、ひいてはグループ参加証を不正に発行することが可能となる。このときグループメンバには不正なグループ参加証発行許可証やグループ参加証と正規のものを判別することはできない。このような場合には、グループ公開鍵・秘密鍵のペアを更新する以外に不正を防ぐ方法はない。一方、グループ管理者がグループ公開鍵・秘密鍵をそれぞれKG__P'、KG__S'に更新したとしても、従来のグループ公開鍵KG__Pとそれに基づいて作成されたグループ参加証発行許可証を持つグループメンバ同士では前記 6. のグループ認証は互いに可能なままなので、グループメンバは常に最新のグループ公開鍵を保持しておく必要があると同時に、最新のグループ公開鍵に対応したグループ参加証を入手する必要がある。発行者はこれに加えて最新のグループ鍵に対応したグループ参加証発行許可証を入手する必要がある。

【 0 1 6 5 】

最新のグループ公開鍵の保持は、第一の実施の形態同様、例えば次のいずれかのような方法により可能である。

【 0 1 6 6 】

(1) グループ管理者がグループ公開鍵・秘密鍵を更新した時点で、図 1 5 に例示したような P 2 P ネットワークを介してネットワーク参加者全員に新しいグ

グループ公開鍵を送付する。対応するグループのメンバは、この新しいグループ公開鍵で自分が保持しているグループ公開鍵を置き換える。

【0167】

(2) 前記2. で告知されるグループ情報に、グループ公開鍵の更新時刻に関する情報も含めておき、前記各グループメンバはグループ公開鍵に加えてこのグループ公開鍵の更新時刻に関する情報も保持しておく。そして、前記6. のグループ認証時には双方が持つグループ公開鍵とその更新時刻の比較を行い、新しい方のグループ公開鍵で古いほうのグループ公開鍵を置き換える。

【0168】

(3) 前記2. の(4)におけるグループ情報インデックスサーバを運営している場合には、グループ情報に(1)同様グループ公開鍵の更新時刻に関する情報も含めておき、グループメンバはオンラインになった時、一定時間おき、あるいは前記6. のグループ認証を行う直前、などのタイミングで前記グループ情報インデックスサーバにアクセスして当該グループの最新のグループ公開鍵を入手する。

【0169】

最新のグループ公開鍵に対応したグループ参加証発行許可証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼(前記10.)を実行すればよい。

【0170】

最新のグループ公開鍵に対応したグループ参加証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼(前記10.)を実行すればよい。

【0171】

次に、前記3. で概要を説明したグループ発行者の追加処理の流れについて、図5と図6を参照して順を追って詳細に説明する。図5はグループ管理者Aとグループ発行者Bでそれぞれ実行される処理の流れを図示したものである。図6はグループ発行者の追加処理が終了した後、グループ発行者が保持する情報を表している。

【0172】

[ステップ501]

事前に、グループ管理者Aはグループの公開鍵KG__P・秘密鍵KG__Sのペアを作成し、このうちグループ公開鍵KG__Pについては公開しておく。

【0173】

[ステップ502]

同じく事前に、発行者候補BXは自分の公開鍵KB__P・秘密鍵KB__Sのペアを作成しておく。これはBが指定した情報（パスフレーズ）を元に生成されたものであってもよいし、プログラムまたは装置が生成した乱数に基づいて生成されたものであってもよい。

【0174】

[ステップ503]

グループ管理者Aは追加するグループ発行者としてユーザBを選択し、Bのアドレス情報を特定する。それは例えば次のような方法で行われる。（1）図15で図示されるP2Pネットワークの情報検索の仕組みを用いて当該グループに参加しているユーザを検索し、該当するユーザがAに対して自分個人を特定する情報と自分のアドレス情報を返信する。Aは受信した情報から、適切と判断するユーザを選択する。（2）電子メールなどP2Pネットワーク以外の手段を含む何らかの手段でBに対してグループ発行者になることを依頼し、Bがそれを受け入れる場合はAに対して自分のアドレス情報を返信する。

【0175】

[ステップ504]

AはBに対してBの公開鍵を送信するよう要求する。

【0176】

[ステップ505]

BはAに対して自分の公開鍵KB__Pを送信する。

【0177】

[ステップ506]

AはBの公開鍵KB__Pに有効期限情報T__Bを添付したものをグループの秘

密鍵で暗号化してグループ参加証許可証 $I_B = e(KB_P + T_B, KG_S)$ を作成し、B に送信する。

【0178】

〔ステップ507〕

B はグループ参加証許可証 I_B を受け取る。

【0179】

これにより、B は他ユーザに対してグループ参加証を発行することが可能になる。本処理後 B が保持する情報は図6に示す通りである。

【0180】

なお、本実施の形態ではグループ管理者AがBに対しグループ発行者の権限を持つよう依頼することとしているが、逆にBの方からグループ発行者の権限をAに対して要求し、Aがそれを承認する形で処理を進めても良い。その場合は、上記ステップ503はBの方からアドレス情報をAに対して通知する処理となる。

【0181】

次に、前記6. で概要を説明したグループへの新規加入依頼処理の流れについて、図7と図8を参照して順を追って詳細に説明する。図7はグループへの新規加入を依頼する加入依頼者Xとグループ発行者Bでそれぞれ実行される処理の流れを図示したものである。図8はグループへの新規加入依頼処理が終了した後、Xが保持する情報を表している。なお、グループ発行者Bは図6に示す情報を保持しているものとする。

【0182】

〔ステップ701〕

X は参加を所望するグループの公開鍵 KG_P を入手し（前記4. 参照）、またグループ発行者Bを特定する（前記5. 参照）。

【0183】

〔ステップ702〕

X は任意の文字列Sを作成し、Bに送信してグループへの新規加入を依頼する。SはXが入力した文字列そのものであってもよいし、プログラムまたは装置が生成した乱数に基づく文字列であってもよい。

【0184】

[ステップ703]

BはSを自分の秘密鍵 KB_S で暗号化した $S' = e(S, KB_S)$ とグループ参加証発行許可証 I_B をXへ送信する。

【0185】

[ステップ704]

Xは I_B をグループ公開鍵 KG_P で復号し、Bの公開鍵 KB_P と有効期限 T_B を得る。

【0186】

[ステップ705]

Xは I_B が KG_P により正常に復号されたことを確認する。正常に復号されない場合は、Bの持つグループ参加証発行許可証 I_B がグループ管理者がグループ秘密鍵 KG_S で暗号化したものであること、すなわちBがグループ発行者であることが確認できないのでXはグループへ新規加入しないまま処理を終了する。

【0187】

[ステップ706]

Xは次いで S' をBの公開鍵 KB_P で復号する。

【0188】

[ステップ707]

Xは S' が KB_P により正常に復号され、かつその結果が元の文字列Sに等しいことを確認する。これにより、 S' がBの公開鍵 KB_P に対応する秘密鍵 KB_S によって暗号化されたこと、すなわちBが確かに秘密鍵 KB_S を保持するグループ管理者であることが確認できる。復号が失敗あるいは復号結果がSに等しくない場合はBがグループ発行者であることが確認できないのでXはグループへ新規加入しないまま処理は終了する。

【0189】

[ステップ708]

XはBに自分の公開鍵 KX_P を送信する。

【0190】

[ステップ709]

BはXのグループ参加証を作成し、Xに送付する。参加証は、Xの公開鍵 KX_P に参加証の効果が消滅する日時 T_X を添付したもの（以下“+”で表記）をBの秘密鍵 KB_S で暗号化して作成したものであり、

$$C_X = e(KX_P + T_X, KB_S)$$

と表せる。 KX_P への T_X の添付方法は、両者がまとめて暗号化されていて復号前には分離不可能であり、一方復号時にはそれぞれを分離することが可能であればどのような方法であってもよい。例えば KX_P 、 T_X をそれぞれ文字列表現したものを所定の分離文字を介して文字列結合したものが考えられる。

【0191】

[ステップ710]

Xはグループ参加証 C_X を受け取り、グループへの新規加入処理が完了する。グループへの新規加入が完了した時点でXが保持する情報は図8に示す通りである。

【0192】

なお、本実施の形態では前記ステップ708においてXの公開鍵をBに対して送信することとしているが、これは前記ステップ702の時点で送信してもよい。

【0193】

また、第一の実施の形態におけるグループへの新規加入依頼同様、前記ステップ702の時点でXがBに対して自分個人を特定できる情報も加えて送信し、Bはその個人を特定できる情報に基づいてXを加入させるかどうか判断し、加入させない場合はXを加入させることなく処理を終了することとしてもよい。

【0194】

次に、前記7.で概要を説明したグループメンバー間の認証処理の流れについて、図10を参照して順を追って詳細に説明する。図10はグループ参加証を既に入手した二人のグループ参加者Xとグループ参加者Yでそれぞれ実行される処理

の流れを図示したものである。なお、XとYはそれぞれ図8と図9に示す情報を保持しているものとする。

【0195】

ステップ1001およびステップ1002は第一の実施の形態における前記ステップ301および前記ステップ302と同様であるので詳しい説明は省略する。

【0196】

【ステップ1003】

Xは、Sを自分の秘密鍵 KX_S で暗号化した文字列 $S' = e(S, KX_S)$ を作成し、 S' 、グループ発行者から受け取ったグループ参加証発行証明書 I_B およびグループ参加証 C_X をYに送信する。

【0197】

【ステップ1004】

Yは、グループ参加証発行証明書 I_B をグループ公開鍵 KG_P で復号し、グループ発行者の公開鍵 KB_P およびグループ参加証発行証明書の有効期限 T_B を得る。

【0198】

【ステップ1005】

Yは、前記ステップ1004で復号が成功したことおよび得られた有効期限 T_B が過ぎていないことを確認する。復号が失敗した場合はグループ参加証発行許可証が正しくグループ秘密鍵 KG_S で暗号化されていないことを意味し、また有効期限が過ぎていればグループ参加証発行許可証が無効であることを意味するので、いずれもXはグループに属していないとみなされ処理は終了する。

【0199】

【ステップ1006】

Yは、Xのグループ参加証 C_X をグループ発行者の公開鍵 KB_P で復号し、Xの公開鍵 KX_P およびXのグループ参加証の有効期限 T_X を得る。

【0200】

【ステップ1007】

Yは、前記ステップ1006で復号が成功したことおよび得られた有効期限T__Xが過ぎていないことを確認する。復号が失敗した場合はグループ参加証がグループ発行者の秘密鍵KB__Sで暗号化されていないことを意味し、また有効期限が過ぎていればグループ参加証が無効であることを意味するので、いずれもXはグループに属していないとみなされ処理は終了する。

【0201】

〔ステップ1008〕

次にYは、S' をXの公開鍵KX__Pで復号する。

【0202】

〔ステップ1009〕

Yは、前記ステップ1008で復号が成功したことおよび復号結果がSに一致することを確認する。復号が失敗した場合および復号結果がSに一致しない場合はXが公開鍵KX__Pに対応する秘密鍵KX__Sを持っていないことを意味するので、Xは第三者の成りすましの可能性があるとみなされ処理は終了する。

【0203】

〔ステップ1010〕

Yは以下のことが全て確認できたので、Xをグループ参加者であると認証する。
(1) グループ参加証の有効期限は切れていない。
(2) Xはグループ参加証に暗号化されていた公開鍵KX__Pに対応する秘密鍵KX__Sを保持している。
(3) グループ参加証を発行したグループ発行者のグループ参加証発行証明書の有効期限は切れていない。
(4) グループ参加証を発行したグループ発行者は、グループ参加証発行証明書に暗号化されていた公開鍵KB__Pに対応する秘密鍵KB__Sを保持している。
(5) グループ参加証発行証明書は、グループ管理者によってグループ秘密鍵KG__Sによって暗号化されたものである。

【0204】

次に、前記ステップ1002から前記ステップ1010までを、XとYの立場を入れ替えて実行する。この処理が成功すれば、XはYをグループ参加者であると認定し、相互の認定が完了する。

【0205】

次に、前記9. で概要を説明したグループ参加証の更新処理の流れについて、図11と図12を参照して順を追って詳細に説明する。図11はグループ参加証の更新を依頼する参加証更新依頼者Xとグループ発行者Bでそれぞれ実行される処理の流れを図示したものである。図12はグループ参加証の更新処理が終了した後、Xが保持する情報を表している。なお、Xは事前に図8に示す情報を、Bは図6に示す情報を保持しているものとする。

【0206】

[ステップ1101]

Xはグループ発行者Bを特定する（前記5. 参照）。なお、ここではグループ発行者としてBを特定したが、同じグループのグループ発行者であれば誰でも以降の処理は成立する。

【0207】

ステップ1102～ステップ1108は前記ステップ702～前記ステップ708と同一であるので説明を省略する。

【0208】

[ステップ1109]

BはXの新たなグループ参加証を作成し、Xに送付する。すなわち、Xの公開鍵 KX_P に新たな有効期限 T_X' を添付したものをBの秘密鍵 KB_S で暗号化して作成した $C_X' = e(KX_P + T_X', KB_S)$ が新たなグループ参加証となる。

【0209】

[ステップ1110]

Xは更新されたグループ参加証 C_X' を受け取り、グループ参加証の更新処理が完了する。グループ参加証の更新処理が完了した時点でXが保持する情報は図12に示す通りである。

【0210】

次に、前記10. で概要を説明したグループ参加証発行許可証の更新処理の流れについて、図13と図14を参照して順を追って詳細に説明する。図13はグループ参加証発行許可証の更新を依頼するグループ発行者Bとグループ管理者A

でそれぞれ実行される処理の流れを図示したものである。図14はグループ参加証発行許可証の更新が終了した後、Bが保持する情報を表している。

【0211】

[ステップ1301]

グループ発行者Bはグループ管理者Aを特定する。第一の実施の形態の処理4で例示した方法と同じ方法で行われる。

【0212】

[ステップ1302]

Bは任意の文字列Sを作成し、Aへ送付して参加証発行許可証の更新を依頼する。SはBが入力した文字列そのものであってもよいし、プログラムまたは装置が生成した乱数に基づく文字列であってもよい。

【0213】

[ステップ1303]

AはSをグループ秘密鍵 KG_S で暗号化した $S' = e(S, KG_S)$ を作成しBへ送信する。

【0214】

[ステップ1304]

Bは S' をグループ公開鍵 KG_P で復号する。

【0215】

[ステップ1305]

Bは S' が KG_P により正常に復号され、かつその結果が元の文字列Sに等しいことを確認する。これにより、 S' がグループ公開鍵 KG_P に対応する秘密鍵 KG_S によって暗号化されたこと、すなわちAが確かにグループ秘密鍵 KG_S を保持するグループ管理者であることが確認できる。復号が失敗あるいは復号結果がSに等しくない場合はAがグループ管理者であることが確認できないので、Bはグループ参加証発行許可証を更新することなく処理は終了する。

【0216】

[ステップ1306]

BはAへ自分の保持するグループ参加証発行許可証 I_B を送信する。

【0217】

[ステップ1307]

AはI__Bをグループ公開鍵KG__Pで復号し、Bの公開鍵KB__Pを得る。

【0218】

[ステップ1308]

Aは前記ステップ1307で復号が成功したことを確認する。復号が成功した場合は、Bが持つグループ参加証発行許可証がグループ秘密鍵KG__Sで暗号化されたものであること、すなわちBが正当なグループ発行者であることが確認できる。復号が失敗した場合は、Bが正当なグループ発行者であることを確認できないのでBのグループ参加証発行許可証は更新されないまま処理は終了する。

【0219】

[ステップ1309]

AはBの公開鍵KB__Pを新たな有効期限T__B'と共にグループ秘密鍵KG__Sで暗号化して更新されたグループ参加証発行許可証I__B' = $e(KB__P + T__B', KG__S)$ を作成し、Bに送信する。

【0220】

[ステップ1310]

Bは更新されたグループ参加証発行許可証I__B'を受け取る。この時点でBが保持する情報は図14に示す通りである。

【0221】

なお、本実施の形態において、グループ参加証発行証明書には有効期限をもうけているが、さらに前記処理11.で述べたグループメンバの失効者情報同様、グループ発行者の失効情報を作成・共有・除外および許可証更新の拒否を行うことで、あるグループ発行者の参加証発行権限を直ちに剥奪することも可能である。

【0222】

本第二の実施の形態独自の効果としては、グループ参加証を発行できるグループ発行者をグループ管理者が必要に応じて設けることにより、秘匿性の高いグループ秘密鍵を複製することなくユーザのグループへの新規加入の機会を増やすこ

とができる点があげられる。

【0223】

なお、第一及び第二の実施の形態では、グループ参加証、グループ参加証発行許可証、あるいは失効リストをグループ管理者あるいはグループ発行者の秘密鍵で暗号化することとしているが、暗号化される内容は公開されている公開鍵および有効期限情報などであって必ずしも秘匿すべき内容ではないので、暗号化する代わりに前記秘密鍵で署名を行うこととしてもよい。この場合でも、受信者は内容の改ざんあるいは不正な発行を検出することができるので、本発明の効果には影響がない。

【0224】

また、第一、第二の実施の形態共に参加証に添付する有効期限は参加証の効果が消滅する日時を示すものとしたが、参加証には参加証の発行日時を添付しておき、有効期限を確認する前記ステップ307では現在日時と発行日時の差分を取り、所定の期間、例えば1ヶ月、を超えていなければ有効期限内であると判断する方法でもよい。

【0225】

さらに、有効期限の判定に利用される現在日時は通常装置のクロックから取り出されるが、グループ認証を行うユーザのそれぞれのクロックが大きく乖離しているとグループ認証処理に影響を及ぼす可能性があるため、双方のクロックが大きくずれた状態でグループ認証処理を行うことは望ましくない。この課題に対しては、グループ認証を行う前に互いのクロックを比較し、所定の基準より大きくずれている場合にはユーザに対して警告を発してグループ認証処理を行わない方法、あるいはどちらか一方のクロックに強制的に他方のクロックを合わせる方法、あるいは双方のクロックの平均値を取って双方ともそれに合わせる方法、などにより対処することが考えられる。

【0226】

さらに、第一の実施の形態の前記処理7、および第二の実施の形態の前記処理8、以外においては通信路の暗号化について言及していないが、全処理について第一の実施の形態の前記処理7、と同様情報転送の暗号化処理を施してもよい。

やり取りされるグループ参加証やグループ参加証発行許可証などは、それを第三者が入手してもメンバあるいはグループ発行者の秘密鍵をも入手しない限りは直ちに不正使用することはできないためこの暗号化処理は必須ではないが、よりセキュリティを高めるために通信路の暗号化を導入することは可能である。

【0227】

さらに、複数のグループ公開鍵・グループ秘密鍵のペアを作成・保持することにより、同一ユーザが複数のグループの管理者となることが可能であるの言うまでもない。同様に複数グループのそれぞれの参加証あるいは参加証発行許可証を保持することにより、同一ユーザが複数グループのそれぞれメンバあるいは発行者となることが可能であるし、同一ユーザが複数のグループに対して異なる権限を持つメンバすなわち管理者・発行者・一般メンバのいずれかとして属することも可能である。

【0228】

【発明の効果】

本発明によれば、以下の利点を持つネットワーク上のグループ管理が可能となる。すなわち、（１）常時稼動しているサーバの運用が不要であり、（２）グループ管理者を含む各グループメンバのオンライン・オフライン状態によらず、グループメンバ間で互いにグループメンバであることの認証が常に可能である。これにより、グループでのみ共有している情報をグループ外のメンバへ漏洩する恐れなく安全に共有することが可能になる。

【図面の簡単な説明】

【図１】

第一の実施の形態におけるグループへの新規加入処理の流れを示した図

【図２】

第一の実施の形態においてグループ参加者Xが保持している情報を示した図

【図３】

第一の実施の形態におけるグループ参加者同士による認証処理の流れを示した図

【図４】

第一の実施の形態におけるグループ参加証の更新処理の流れを図示した図

【図 5】

第二の実施の形態におけるグループ発行者の追加処理の流れを図示した図

【図 6】

第二の実施の形態においてグループ発行者 B が保持する情報を示した図

【図 7】

第二の実施の形態におけるグループへの新規加入処理の流れを図示した図

【図 8】

第二の実施の形態においてグループ参加者 X が保持している情報を示した図

【図 9】

第二の実施の形態においてグループ参加者 Y が保持している情報を示した図

【図 1 0】

第二の実施の形態におけるグループ参加者同士で行われる認証処理の流れを示した図

【図 1 1】

第二の実施の形態におけるグループ参加証の更新処理の流れを示した図

【図 1 2】

第二の実施の形態においてグループ参加証を更新したグループ参加者 X が保持している情報を示した図

【図 1 3】

第二の実施の形態におけるグループ参加証発行許可証の更新処理の流れを示した図

【図 1 4】

第二の実施の形態においてグループ参加証発行許可証を更新したグループ発行者 B が保持している情報を示した図

【図 1 5】

P 2 P ネットワークに参加しているユーザ間での情報転送の流れを表した概念図

【図 1 6】

P2Pネットワークにおけるグループ管理の問題点を表した図

【符号の説明】

101～112 第一の実施の形態におけるグループへの新規加入処理の各ステップ

301～310 第一の実施の形態におけるグループ参加者同士による認証処理の各ステップ

401～410 第一の実施の形態におけるグループ参加証の更新処理の各ステップ

501～507 第二の実施の形態におけるグループ発行者の追加処理の各ステップ

701～710 第二の実施の形態におけるグループへの新規加入処理の各ステップ

1001～1010 第二の実施の形態におけるグループ参加者同士による認証処

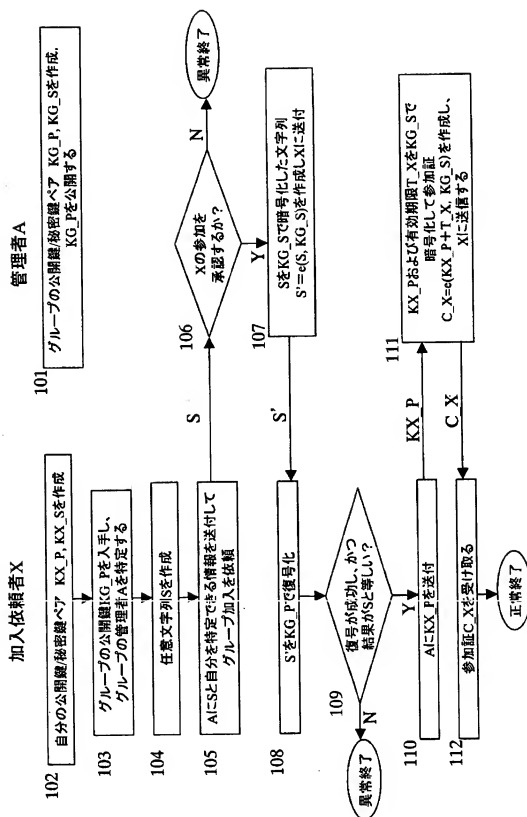
1101～1110 第二の実施の形態におけるグループ参加証の更新処理の各ス

1301～1310 第二の実施の形態におけるグループ参加証発行許可証の更新処理の各ステップ

【書類名】

図面

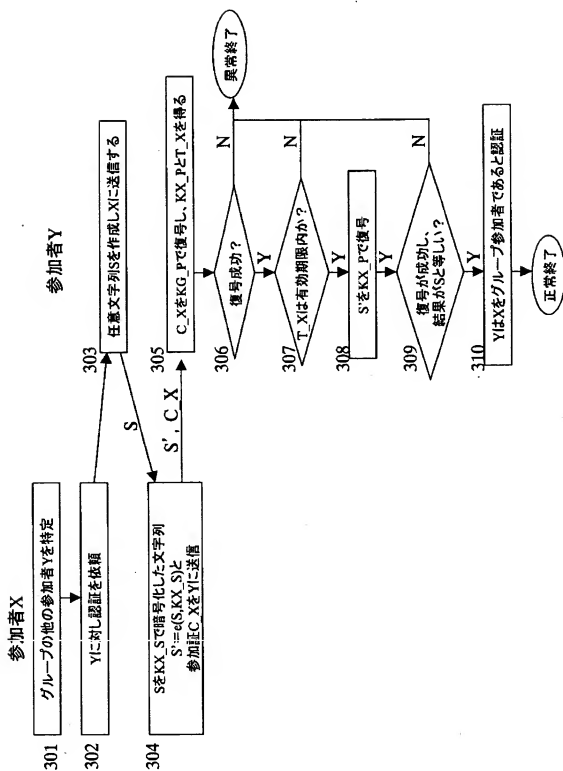
【図1】



【図2】

KX_P: Xの公開鍵
KX_S: Xの秘密鍵
KG_P: グループの公開鍵
 $C_X = e(KX_P + T_X, KG_S)$: Xのグループ参加証

【図 3】



【图4】

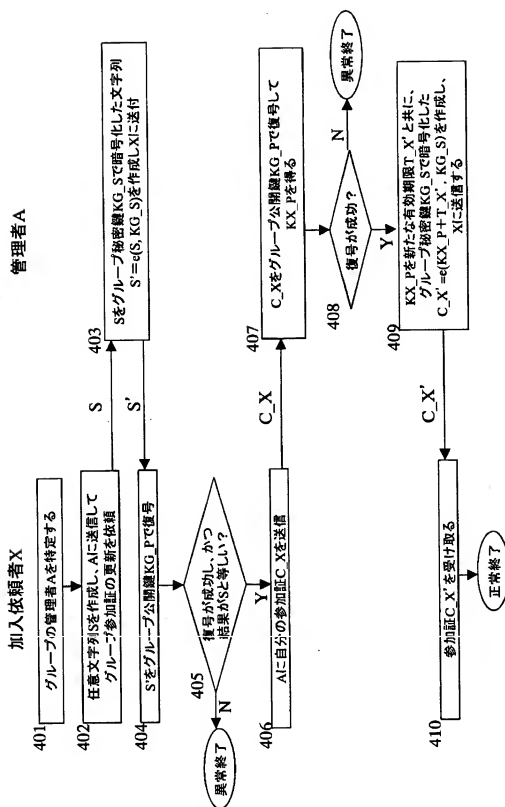
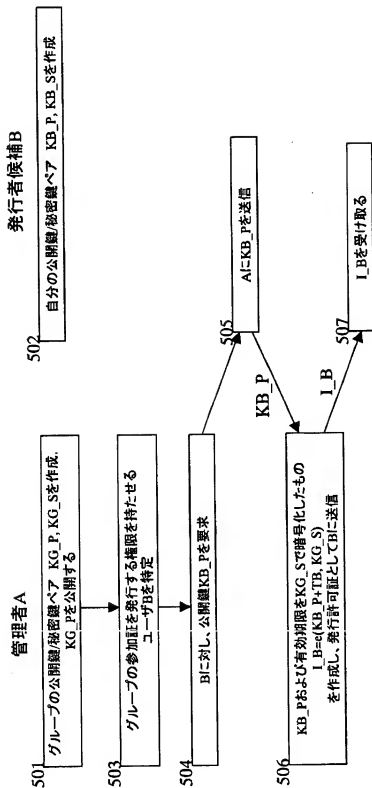


図 5



【図 6】

KB_P : B の公開鍵
 KB_S : B の秘密鍵
 KG_P : グループの公開鍵
 $I_B = e(KB_P + T_B, KG_S)$
 I_B : B のグループ参加証発行許可証

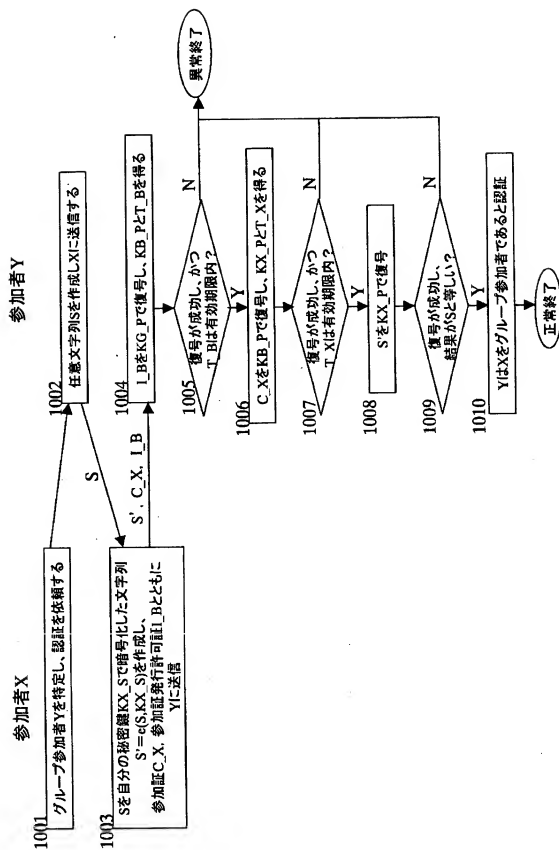
【図8】

KX_P : Xの公開鍵
 KX_S : Xの秘密鍵
 KG_P : グループの公開鍵
 $I_B = e(KB_P + T_B, KG_S)$
 : Bのグループ参加証発行許可証
 $C_X = e(KX_P + T_X, KB_S)$: Xのグループ参加証

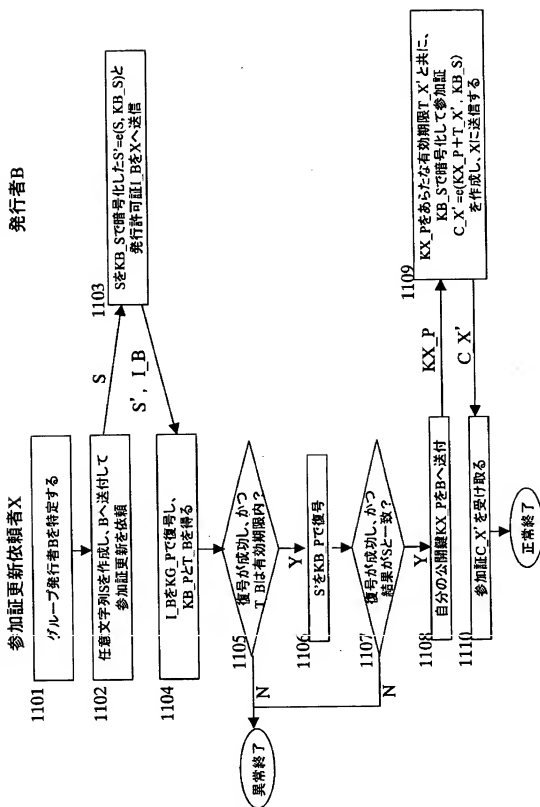
【図9】

KY_P : Yの公開鍵
 KY_S : Yの秘密鍵
 KG_P : グループの公開鍵
 $I_C = e(KC_P + T_C, KG_S)$
 : 別の発行者Cのグループ参加証発行許可証
 $C_Y = e(KX_P + T_X, KB_S)$
 : Cが発行したYのグループ参加証

【図10】



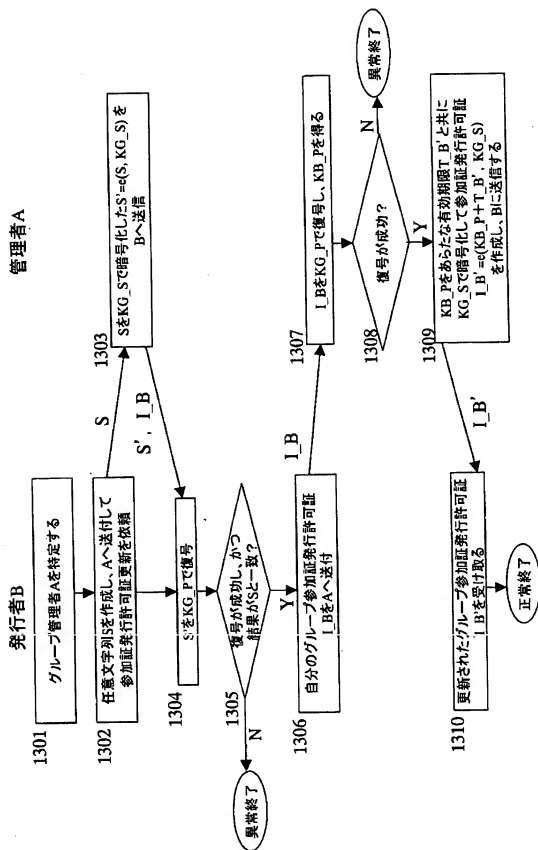
【図 11】



【図 1 2】

KX_P : X の公開鍵
 KX_S : X の秘密鍵
 KG_P : グループの公開鍵
 $I_B = e(KB_P + T_B, KG_S)$
 I_B : B のグループ参加証発行許可証
 $C_X = e(KX_P + T_X', KB_S)$: X のグループ参加証

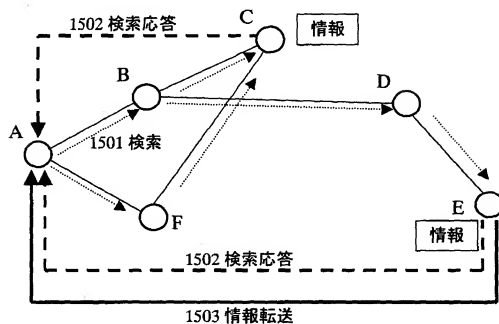
【図13】



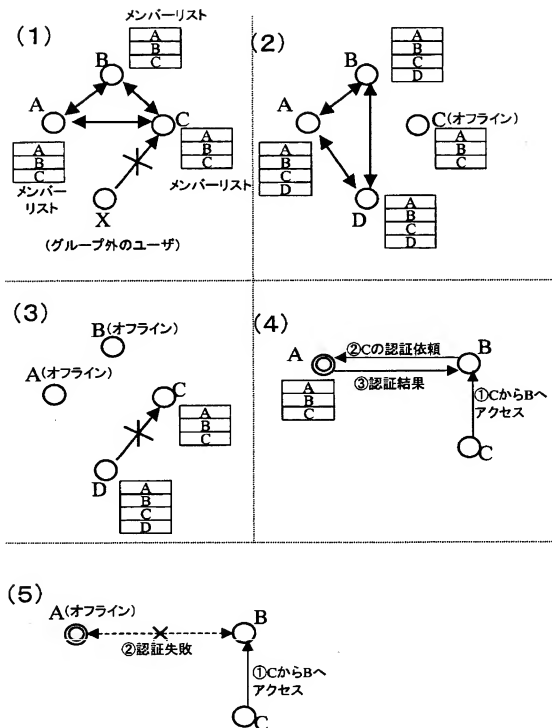
【図14】

KB_P: Bの公開鍵
 KB_S: Bの秘密鍵
 KG_P: グループの公開鍵
 $T_{B'} = e(KB_P, T_{B'}, KG_S)$
 : Bのグループ参加証発行許可証

【図15】



【図16】



【書類名】 要約書

【要約】

【課題】 常時稼動するサーバの運用が不要であり、常に任意のメンバ間で互いに認証が可能。

【解決手段】 管理者あるいは発行者が発行する参加証に基づいてグループメンバ間で互いにグループに属することを認証する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社